Г. А. Бузов

Защита информации ограниченного доступа от утечки по техническим каналам

Горячая линия–Телеком

Г. А. Бузов

Защита информации ограниченного доступа от утечки по техническим каналам

Москва
Горячая линия - Телеком
2015

УДК 681.3.067
ББК 32.81
Б90

Бузов Г. А.

Б90 Защита информации ограниченного доступа от утечки по техническим каналам. – М.: Горячая линия – Телеком, 2015. – 586 с., ил.

ISBN 978-5-9912-0424-8.

Систематизированы обширные теоретические и практические сведения в области организации и осуществления работ по защите от утечки информации по техническим каналам. Рассмотрены возможные технические каналы утечки как речевой, так и обрабатываемой техническими средствами информации. Приведены результаты краткого анализа основных характеристик и особенностей функционирования современной аппаратуры защиты информации и поиска закладочных устройств (ЗУ). Рассмотрен пакет нормативно-методических документов регламентирующих деятельность в области защиты информации. Приведены методики принятия решения на защиту от утечки информации, а также выполнения различных видов специального контроля и проверок при проведении поисковых мероприятий. Рассмотрены подходы к методике измерений в ходе проведения специсследований в современных условиях и требования к используемой для этих целей аппаратуре.

Для специалистов, работающих в области защиты информации, руководителей и сотрудников аттестационных центров и служб безопасности предприятий, а также студентов и слушателей курсов повышения квалификации.

ББК 32.81

Адрес издательства в Интернет www.techbook.ru

Бузов Геннадий Алексеевич
Защита информации ограниченного доступа от утечки по техническим каналам
Справочное издание

Предисловие

Современный этап развития общества характеризуется существенным возрастанием понимания роли и актуальности проблем обеспечения безопасности во всех сферах жизнедеятельности. Особенно показателен этот процесс для сферы информационной безопасности, которая за последнее десятилетие вышла из области компетенции сугубо специальных служб и превратилась в мощный сегмент рыночной индустрии современных информационно-телекоммуникационных технологий.

При мощном прогрессе области технической защиты информации общепризнано, что безопасность функционирования сложных организационно-технических систем определяется, прежде всего, так называемым человеческим фактором, в качестве одной из характеристик которого выступает уровень профессиональной подготовки работников. Проведенные теоретико-методологические исследования проблем информационной безопасности позволили сделать вывод, что задача создания системы планомерной подготовки, переподготовки и повышения квалификации кадров играет не менее важную роль наряду с технологическими и техническими аспектами защиты чувствительной (критичной) информации. Актуальность такой задачи не подлежит сомнению в связи с возрастающими требованиями к эффективности, надежности и безопасности сложных комплексов, функционирующих на основе использования сложных современных технологий.

Именно поэтому в Доктрине информационной безопасности Российской Федерации развитие системы обучения кадров, используемых в области обеспечения информационной безопасности, отнесено к числу первоочередных мероприятий по реализации государственной политики в рассматриваемой сфере.

Проблема повышения кадрового потенциала является важнейшей и для государственной системы технической защиты информации. Так, в соответствии с постановлениями Правительства Российской Федерации необходимыми требованиями и условиями осуществления лицензируемых видов деятельности в области технической защиты конфиденциальной информации является наличие у специалистов организации-лицензиата либо соответствующего высшего профессионального образования, либо свидетельства о специальной

переподготовке по вопросам защиты информации. Такие требования введены в связи с наличием определенного дефицита квалифицированных кадров по обеспечению безопасности современных информационных технологий.

Органы государственной власти, в частности Федеральная служба безопасности и Федеральная служба по техническому и экспортному контролю Российской Федерации, как компетентные органы всегда уделяли особое внимание и поддерживали усилия ученых, преподавателей и специалистов по разработке нормативного и методического обеспечения процессов обучения кадров в области технической защиты информации в рамках государственной системы высшего, дополнительного и среднего специального образования. Не секрет, что в настоящее время остро ощущается также дефицит в специализированной литературе для подготовки кадров разных образовательных уровней. Особенно остро это ощущается в различных учебных центрах, занимающихся повышением квалификации специалистов в области технической защиты информации. Имеющаяся в наличии литература пока не охватывает все аспекты рассматриваемой проблемы, а обсуждаемые вопросы часто не имеют достаточной глубины проработки.

В предлагаемом вниманию читателей специализированном учебном пособии автор, используя существующую литературу, свой опыт работы и методические разработки в данной области, последовательно и в необходимом объеме постарался изложить вопросы, касающиеся организации и осуществления работ по защите от утечки информации по техническим каналам.

Введение

Приступая к решению любого вопроса, мы, прежде всего, интересуемся тем, что же нам известно по данному вопросу, то есть собираем необходимые данные или информацию. Однако то, что нам представляется важной информацией, другими, не интересующимися данным вопросом, может восприниматься как никчемный и заурядный шум, поэтому представляется необходимым и актуальным разобраться в том, что же означает термин «информация» и как его трактуют руководящие документы.

В Большой советской энциклопедии этот термин трактуется следующим образом: «Информация (от лат. informatio — разъяснение, изложение) — сведения, передаваемые одними людьми другим людям устным, письменным или каким-либо другим способом (например, с помощью условных сигналов, с использованием технических средств и т. д.), а также сам процесс передачи или получения этих сведений» БСЭ, издание III, том 10, страница 353.

ФЗ № 149 «Об информации, информационных технологиях и защите информации», принятый Государственной Думой 27 июля 2006 года, таким образом трактует это понятие: информация — сведения (сообщения, данные) независимо от формы их представления.

Расширим и уточним, применительно к нашей тематике, понятие информации. Для удобства изложения разделим всю информацию на две основных категории:

- информация вербальная;
- информация невербальная.

Вербальная информация — это различные сведения, выраженные средствами языка (письменно или устно).

Невербальная информация не передает какого-то конкретного содержания, но косвенно указывает, подтверждает или опровергает тот или иной факт. Это перемещения, встречи с кем-то, посещаемые места, поведение при этом и т. д. (например, тайная встреча с представителем конкурирующей фирмы).

Данные категории информации можно условно подразделить на два вида: первый — это (используя американскую терминологию) «мягкая» информация, второй — «твердая» информация.

«Мягкая» информация — это информация, носителем которой является поле (акустическое или электромагнитное). Такая информация живет буквально мгновения; однажды произведенная (озвученная), она исчезает и повторно воспроизведена быть не может. Говоря простым языком, «мягкая» информация — это сведения, которые содержатся в произнесенных вами (по телефону или в личной беседе) словах, или ваши текущие действия.

«Твердая» информация — это информация, записанная на каком-то материальном носителе (бумаге, магнитном носителе, флешкарте и т. п.). Такая информация, если ее специально не стирать, может существовать до тех пор, пока существует сам носитель. К ней можно отнести различные документы, магнитные, кино- и видеозаписи и т. п.

Кроме того, информацию можно условно подразделить на:

- общую, или тотальную, которая позволяет получить общее обзорное представление об интересующей проблеме и участниках (индивидах и организациях) решающих данную проблему;
- текущую, или оперативную, позволяющую постоянно ориентироваться в курсе изменяющихся событий;
- конкретную, т. е. информацию, позволяющую ответить на определенные вопросы и заполнить выявленные пробелы в имеющихся данных;
- косвенную, которая, будучи состыкованной с имеющимися данными по решаемой проблеме только опосредованно, позволяет подтвердить или опровергнуть некие предположения;
- оценочную, позволяющую разобраться и оценить события и дать прогноз относительно их развития в будущем. Это оптимально обработанные данные.

При этом следует конкретно различать и не путать: факты (данные), мнения (личностные предположения) и собственно информацию (аналитически обработанные данные).

Своевременно полученная и достоверная информация обычно позволяет:

- ориентироваться в ситуации;
- четко планировать свои действия;
- отслеживать результативность проводимых акций;
- уклоняться от неожиданностей;
- манипулировать отдельными людьми и группировками.

При этом для получения необходимой информации широко используются её физические свойства. Следовательно, знание особенностей функционирования информации различного вида позволит успешно организовать защиту от её утечки по различным каналам. Что

же мы подразумеваем под утечкой информации? Под утечкой информации понимается несанкционированный процесс переноса информации от источника к злоумышленнику.

Понятие «утечка» широко распространено. Говорят об утечке воды, газа, материальных ценностей со склада, информации и т. д. Утечка информации возможна при ее разглашении людьми, утери ими носителей с информацией, переносе информации с помощью любого вида носителя.

Рассматривая вопрос об особенностях утечки информации, необходимо отметить, что:

- утечка информации может происходить только при попадании ее к заинтересованному в ней несанкционированному получателю (злоумышленнику), в отличие, например, от утечки воды или газа;
- при утечке информации происходит ее тиражирование, которое не изменяет характеристики носителя информации (не уменьшается количество листов документа, не сокращается число пикселей изображения, не меняются размеры, цвет и другие характерные признаки продукциии и т. д.);
- цена информации при ее утечке уменьшается за счет тиражирования;
- факт утечки информации, как правило, обнаруживается спустя некоторое время, по последствиям, когда меры по обеспечению ее безопасности могут оказаться неэффективными.

Следовательно, под утечкой информации следует понимать не процесс распространения носителя информации за пределы определенной области пространства вообще, а частный случай распространения, когда она попадает к злоумышленнику.

Замечание о несанкционированности получателя имеет принципиальное значение. Если получатель информации санкционирован, то речь идет не об утечке, а о передаче информации по так называемому функциональному каналу связи, специально создаваемому для обеспечения коммуникаций в человеческом обществе.

Современный деловой человек не может отмахиваться от проблем доступа к закрытой информации и от вопросов скрытия своей информации. Естественно, не рекомендуется использовать криминальные пути достижения своих целей — заниматься шпионажем для шантажа и вторжения в личную жизнь граждан. Но обязательно необходимо представлять, как это могут сделать другие по отношению к вам.

Обладание одной и той же информацией различными пользователями может привести к абсолютно противоположным результатам. При этом информацию принято считать ценной лишь тогда, когда ее

можно использовать, причем полезность информации сильно зависит от ее полноты, точности и своевременности.

По мнению западных специалистов, утечка 20 % коммерческой информации в шестидесяти случаях из ста приводит к банкротству фирмы. Информация — второй, после времени, по ценности товар. Кто владеет информацией, тот добивается наибольших результатов.

Для уменьшения угроз экономической деятельности фирмы необходимо получение информации о внешней и внутренней среде, а это включает в себя, помимо прочего, информацию о конкурентах, информацию о сотрудниках. Поэтому вполне естественно, что уменьшение данных угроз для одних влечет за собой увеличение угроз экономической деятельности для других.

Получение даже незначительной информации о конкуренте может сэкономить фирме огромные средства, что является достаточно сильным стимулом для нарушения законов, регулирующих отношения в области информации. Сложнее приходится добросовестному субъекту данных отношений, так как он ограничен в своих действиях Законом.

Поэтому знание того, каким путем важная для него информация ограниченного пользования может попасть к конкурентам, позволит собственнику информации организовать ее успешную защиту, а изучение законодательства Вашего государства позволит Вам, не нарушая законов, регламентирующих деятельность в области информационной безопасности, осуществить защиту информации ограниченного пользования, которая циркулирует на Вашем предприятии.

1 ХАРАКТЕРИСТИКИ ТЕХНИЧЕСКИХ КАНАЛОВ УТЕЧКИ ИНФОРМАЦИИ

В различных источниках, как в закрытых, так и открытых, можно встретить различные определения понятия «технический канал утечки». Тем не менее, общий смысл остаётся неизменным — под *техническим каналом утечки информации* (ТКУИ) понимают совокупность источника информации (*передатчик*), линии связи (*протяжённая физическая среда*), по которой распространяется информационный сигнал (собственно канал), и средство приёма (*перехвата*) информации. В качестве средства приёма, перехвата информации (*средства разведки*) подразумеваются как некое техническое средство (приёмник), так и органы чувств человека или их совокупность. Предполагается, что в линии связи (среде распространения) всегда присутствует некий уровень шумов (*помех*), препятствующих правильному приёму сигнала. В большинстве случаев шумы рассматриваются на входе устройства приёма. Так же, как правило, полагают, что уровень этих шумов одинаков на всём протяжении среды распространения.

Источниками (*передатчиками*) информации могут быть непосредственно голосовой аппарат человека, излучатели систем звукоусиления, печатный текст, персональные ЭВМ и т. п.

Сигналы являются материальными носителями информации. По своей природе они могут быть электрическими, электромагнитными, акустическими и другими и представляют собою, как правило, электрические, электромагнитные, акустические и другие виды колебаний (волн), при этом информация содержится в изменениях их параметров. Для того чтобы терминологически отличить их от иных сигналов, не переносящих защищаемую информацию и не являющихся одновременно шумами, в литературе по рассматриваемой проблеме их принято называть опасными сигналами.

В зависимости от своей физической основы сигналы распространяются в различных физических средах. К ним относятся свободное пространство, конструкции зданий, соединительные линии и токопроводящие элементы, грунт (земля) и т. п.

Средства перехвата информации (синоним — *средства разведки или средства технической разведки*) служат для приема и преобразования сигналов с целью получения информации.

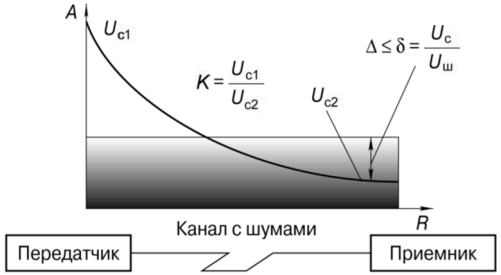


Рис. 1.1. Обобщённая модель технического канала утечки: U_{c1} — величина опасного сигнала на выходе передатчика; U_{c2} — та же величина на входе приёмника (средства разведки); Δ — отношение сигнал/шум на входе приёмника; K — величина, характеризующая ослабление (затухание) опасного сигнала при распространении в канале, кривая иллюстрирует некий закон этого затухания; R — протяжённость (длина) канала от передатчика до приёмника; тонированная полоса иллюстрирует минимальный уровень шумов в канале

Таким образом, наиболее обобщённая модель технического канала утечки информации состоит из трёх основных составляющих — *передатчика, среды передачи* и *приёмника*. Применение такой модели позволяет использовать для анализа весьма развитый аппарат теории передачи информации, классической радиотехники и ряда других областей знаний.

1.1. Модель технического канала утечки

Рассмотрим последовательно основные элементы предлагаемой модели и определим её важные для оценки параметры.

Отметим, что в терминах и понятиях предлагаемой модели полностью отсутствует упоминание (и, соответственно, дифференциация) по физическим основам и формам существования опасного сигнала. Общая модель безотносительна к этому параметру. А для составления перечня физически возможных, реализуемых каналов утечки форма существования сигнала является важнейшей характеристикой.

Как указывалось выше, источником опасного сигнала, передатчиком является некий материальный объект, выполняющий роль носителя, генератора или обработчика защищаемой информации. Именно в этот момент и появляется необходимость определить форму существования защищаемой информации.

Для подавляющего числа объектов защиты физических форм существования защищаемой информации немного, а именно:

- речевая информация в форме акустических, т. е. механических, колебаний в воздушной (газовой) среде;
- речевая информация в форме вибрационных, т. е. механических колебаний, в твердом (жидком) теле;

- речевая информация в форме электрических колебаний (преобразованная, аналоговая и/или цифровая) в проводящей среде;
- информация (неречевая) в электронной форме в виде электрических колебаний (находящаяся на компьютерах, средствах связи и т. д.) в проводящей среде;
- информация в визуальной форме (твёрдые копии документов, изображение на кино-, теле- и/или экране монитора) в виде видимого света (видовая).
- информация в некоторых отдельных, специальных формах (некогерентное ИК излучение, лазерное излучение вне зависимости от длины волны, модулированный ультразвук и т. д.).

Необходимо учитывать, что разделение защищаемой информации на речевую и любую иную носит исторический характер, связанный с исключительно аналоговой формой преобразованной речевой информации на ранних стадиях развития техники и её передачей в форме модулированных сигналов. На сегодняшний день это разделение, особенно для цифровой формы существования информации, носит (во многом, хотя и не во всём) условный характер.

При этом следует особо отметить, что информация, находящаяся на машинных носителях (диски жёсткие, оптические, гибкие, магнитооптические, магнитные ленты, flash-память всех видов) вне процессов считывания/записи (при хранениив статике) в принципе не образует технических каналов утечки.

Естественно, в данном контексте за пределами рассмотрения остаются «экзотические» виды технической разведки и рассматриваемые для них технические каналы (сейсмический, радиологический, гидроакустический и т. д.).

Рассмотрим более детально источники возможных опасных сигналов для основных форм существования защищаемой информации.

Для речевой информации в форме акустических и вибрационных сигналов их только два типа — речевой аппарат человека и/или громкоговоритель (колонка) некой аудиосистемы.

Для речевой информации в форме преобразованной, аналоговой и/или цифровой электрических колебаний в проводящей среде источниками являются широчайший набор различных технических средств (вся техника систем звукоусиления, конференц-систем, звукозаписи, радио- и телевещания и т. д.). В существующих нормативных документах и литературе они объединены аббревиатурой ТСПИ (*технические средства приема/передачи информации*). Кроме того, к этому же типу источников следует отнести и многие виды компьютерной техники, если рассматривается защита оцифрованной речевой информации, ими обрабатываемой. Следует отметить, что в области цифровой, компьютерной техники, обрабатывающей *неречевую* информа-

цию, используется иная аббревиатура с абсолютно тем же смыслом — ОТСС (основные технические средства и системы).

Для информации неречевой в электронной форме набор источников полностью совпадает со второй частью источников (цифровых) для речевой информации в форме электрических колебаний и расширяет его другими типами разнообразных устройств вычислительной техники и не только (представить себе принтер или сканер, обрабатывающий речевую информацию довольно трудно).

Для информации в визуальной форме (твёрдые копии документов, изображение на кино- теле- и/или экране монитора) в форме видимого света (видовая) набор источников уже дан в самом определении.

Для информации в некоторых отдельных, специальных формах (некогерентное ИК излучение, лазерное излучение вне зависимости от длины волны, модулированный ультразвук и т. д.) вопрос источника должен рассматриваться в каждом случае отдельно, общие рекомендации в данном случае затруднены. Это и волоконно-оптические линии связи, и пространственные ИК каналы, и другие, ещё более экзотические источники.

Отметим, что сигнал на выходе передатчика (и, естественно, на входе канала распространения) предполагается не нулевым. В противном случае рассмотрение сразу же теряет смысл, канал утечки не может существовать. Фактически такой вариант полностью эквивалентен отсутствию передатчика.

Рассмотрим второй элемент модели — среду распространения опасного сигнала (канал распространения).

Для *речевой информации в форме акустических сигналов* это воздушная среда (включая воздуховоды систем вентиляции, дымоудаления, любые короба, кабельгоны, трещины, отверстия и т. д.).

Для *речевой информации в форме вибрационных сигналов* это любое твёрдое или жидкое тело (строительные конструкции, трубопроводы, жидкость в свободной форме и/или в трубопроводе и т. д.).

Для *речевой информации в форме электрических колебаний в проводящей среде* это любая токопроводящая среда (провода, кабели, каркасы зданий, металлические части строительных и/или инженерных систем); в ряде случаев, когда опасный сигнал достигает значительных величин и возникает заметное электрическое и/или магнитное поле, — свободное пространство.

Для *информации (неречевой) в электронной форме* среда распространения будет аналогично речевой информации в форме электрических колебаний в проводящей среде, но со значительным преобладанием случаев распространения сигнала в форме поля в свободном пространстве.

Для *информации в визуальной форме* это почти всегда исключительно свободное пространство в условиях прямой видимости.

Для *информации в некоторых отдельных, специальных формах* это может быть свободное пространство и некоторые иные среды, анализируемые в конкретных случаях.

Важнейшими параметрами среды распространения как элемента модели являются:

- *затухание сигнала* от начала к концу, зависящее от погонного затухания и длины канала;
- *уровень помех* в канале.

Для понимания сущности явления более детально рассмотрим данный вопрос. Так как любой физически реализуемый канал передачи информации (именно так рассматривается канал утечки) имеет некоторый уровень шумов (помех), который принимается постоянным, и, одновременно, некоторое погонное затухание для распространяющегося сигнала, то при постоянном уровне шума, чем длиннее канал, тем меньше отношение сигнал/шум на входе средства разведки. Кроме того, для всех каналов, среда распространения которых ограничена искусственными, техногенными границами (конструкции зданий, трубопроводы, воздуховоды, проводные линии, практически всё, кроме свободного пространства), необходимым условием существования (образования) ТКУИ является доступ потенциального противника к среде распространения. При этом среда распространения сигнала должна быть непрерывна от передатчика до точки приёма. Как правило, возможности потенциального противника вместе со средством разведки ограничены. Он не может проникнуть в хорошо охраняемую зону вокруг объекта разведки. Эту зону можно условно назвать контролируемой зоной (КЗ). Контролируемая зона — это пространство (территория, здание, часть здания), в котором исключено неконтролируемое пребывание сотрудников и посетителей организации, а также транспортных, технических и иных материальных средств. По определению КЗ приёмник (средство разведки) не может оказаться внутри её, а предполагается, что он может находиться, в наихудшем случае, на границе КЗ. Проведенный анализ позволяет сделать важный вывод о том, что если среда распространения не имеет выхода за пределы КЗ, то ТКУИ не может существовать (образоваться). Из этого правила есть лишь небольшое число исключений, которые будут рассмотрены позднее. С точки зрения математики данный вариант является предельным и эквивалентен ситуации с бесконечно большим затуханием в канале.

Последним элементом модели является приёмник как средство перехвата, средство разведки и т. д. Единственным (и нормированным) параметром приёмника является его чувствительность, ограни-

ченная собственными шумами. Его значения, как правило, задаются регламентирующими документами. В математических терминах вариант отсутствия приёмника эквивалентен приёмнику с нулевой чувствительностью. Более подробное рассмотрение приёмника опустим, так как это уже вопрос, относящийся к закрытым областям знаний. Важно знать, что приёмник реально существует и есть нормативная документация, которая устанавливает его параметры для каждого ТКУИ.

Таким образом, проведенная суммарная качественная математическая оценка условий существования (образования) канала утечки позволяет сделать вывод о том, что для существования технического канала утечки необходимым и достаточным условием является наличие:

- передатчика с ненулевой мощностью сигнала на выходе;
- среды распространения с конечным уровнем помех, конечной длиной и конечным погонным затуханием, обеспечивающей достаточное отношение сигнал/шум на выходе канала (входе приёмника);
- приёмного устройства с достаточной для приёма этого сигнала чувствительностью.

Предельные значения основных параметов любого из этих элементов приводят к невозможности даже потенциального существования канала утечки. Такими значениями, например, являются нулевой сигнал на выходе передатчика, бесконечное затухание в канале, нулевая чувствительность приёмника (фактически отсутствие любого из перечисленных элементов). Следует обратить внимание на то, что любую комбинацию перечисленных условий можно свести к одному, единому параметру. В качестве этого параметра выступает отношение сигнал/шум при условии заданной чувствительности средства перехвата (разведки) на входе приёмника. Именно эта величина является для подавляющего числа каналов утечки основным (прямо или косвенно заданным) нормированным параметром, *параметром защищённости*, по измеренному (рассчитанному) значению которого принимается решение о степени защищённости объекта. Для некоторых каналов приняты параметры защищённости иной физической природы, но и в этих случаях они вычисляются из отношения сигнал/шум.

1.2. Потенциально возможные технические каналы утечки информации

В зависимости от физической природы возникновения информационных сигналов, а также среды их распространения и способов перехвата, технические каналы утечки информации можно условно разделить на *электромагнитные, электрические, акустические, вибрационные* и *видовые.*

При анализе технических каналов утечки информации ТСПИ и ОТСС необходимо рассматривать как систему, включающую основное оборудование, оконечные устройства, соединительные линии (совокупность проводов и кабелей, прокладываемых между отдельными ТСПИ (ОТСС) и их элементами), распределительные и коммутационные устройства, системы электропитания, системы заземления.

Наряду с ТСПИ (ОТСС) в помещениях устанавливаются технические средства и системы, непосредственно не участвующие в обработке защищаемой информации, но использующиеся совместно с ТСПИ (ОТСС) и находящиеся в зоне электрических или магнитных полей, создаваемых ТСПИ (ОТСС) или под воздействием речевого защищаемого сигнала. Такие технические средства и системы обозначаются аббревиатурой ВТСС (вспомогательные технические средства и системы). Это технические средства открытой телефонной и громкоговорящей связи, системы пожарной и охранной сигнализации, средства и системы кондиционирования, электрификации, радиофикации, часофикации, электробытовые приборы, персональные ЭВМ (и их компоненты) и т. д.

В последующем изложении, за исключением отдельно оговариваемых случаев, мы будем рассматривать естественные каналы утечки, т. е. возникающие за счёт свойств материалов, узлов и элементов технических средств без специально предпринятых для этого потенциальным противником усилий. Применение специально созданных и внедрённых в технические средства, помещения, предметы интерьера и т. д. устройств, предназначенных для приёма, запоминания и передачи информации (*закладочных устройств*), которые образуют *искусственные* ТКУИ, будет рассматриваться отдельно.

1.2.1. Технические каналы утечки речевой информации (акустическая речевая разведка)

Как следует из названия раздела, целью данного вида разведки является получение информации, содержащейся в человеческой речи (непосредственно произносимой либо воспроизводимой техническими средствами).

Речевой сигнал — сложный акустический сигнал, основная энергия которого сосредоточена в диапазоне частот от 175 до 5600 Гц.

Голосовой аппарат человека или громкоговоритель (колонка) является *первичным* источником акустических колебаний, которые представляют собой возмущения воздушной среды в виде волн сжатия и растяжения (продольных волн).

При обмене речевой информацией возникающие акустические колебания действуют на ограждающие строительные конструкции, инженерные системы помещений, на расположенные в помещении технические средства, в которых находится речевой источник. При этом в

них возникают вибрационные колебания. Под воздействием вибраций на узлы, блоки, элементы электрической и электронной аппаратуры в её цепях и отходящих линиях возникают пропорциональные звуковому давлению электрические сигналы (*акустоэлектрический, «микрофонный» эффект*).

При одновременном воздействии акустических колебаний и внешнего (генерируемого средством разведки потенциального противника) высокочастотного сигнала на узлы, блоки, элементы электрической и электронной аппаратуры в её цепях и отходящих линиях или пространстве возникают ВЧ сигналы, модулированные речевым сигналом (*ВЧ навязывание* и/или *ВЧ облучение*).

Таким образом, в своем первоначальном состоянии речевой сигнал в помещении присутствует в виде акустических колебаний. Следовательно, вибрации, электрические сигналы звукового диапазона, модулированные ВЧ сигналы являются уже результатом преобразования первоначальных акустических колебаний.

В зависимости от физической природы и среды распространения прямого или преобразованного сигналов и способов их перехвата технические каналы утечки речевой информации можно разделить на:

- акустические и вибрационные (акустика и виброакустика, АВАК);
- акустоэлектрические (АЭП);
- ВЧ навязывание (ВЧН);
- ВЧ облучение (ВЧО);
- паразитную высокочастотную генерацию.

Акустический канал. В акустическом канале утечки информации средой распространения речевых сигналов является воздух, и для приёма (перехвата) сигнала используются органы слуха человека либо первичные преобразователи — микрофоны (в том числе направленные), которые соединяются с усилительными и звукозаписывающими устройствами. Вариант существования ТКУИ без применения технических средств перехвата в нормативной документации носит условное наименование «непреднамеренное прослушивание».

В рамках сегодняшних подходов различают два подвида ТКУИ с применением технических средств разведки (для акустической информации):

- перехват в режиме реального времени («реал тайм») с прямым прослушиванием сигнала на выходе средства перехвата;
- отложенную обработку сигнала, подразумевающую его запись с последующей шумоочисткой, математической обработкой и т. д., повышающих вероятность правильного восстановления информации.

Необходимо отметить, что непреднамеренное прослушивание относится к единственному исключению среди набора наиболее вероят-

ных ТКУИ, так как принято, что оно может осуществляться и внутри КЗ.

Вибрационный канал. Прежде всего обратим внимание читателя на существование терминологически неверного, но распространённого синонима — «виброакустика, виброакустический канал». В вибрационных технических каналах утечки информации средой распространения сигнала являются ограждающие строительные конструкции помещений (стены, потолки, полы) и инженерные системы помещений (трубопроводы (и жидкость в них) водоснабжения, отопления, корпуса коробов вентиляции и т. п.). Для приёма (перехвата) речевых сигналов в этом случае используются первичные преобразователи — акселерометры, велосиметры и тензометры. Отдельно рассматривается (в качестве отдельного типа ТКУИ) вариант вибрационного канала утечки, в котором в качестве первичного преобразователя применяется лазерный акселерометр. В этом варианте съём вибраций строительной конструкции, например оконного остекления или другого отражающего предмета, находящегося под воздействием акустического сигнала, осуществляется дистанционно, из-за границы контролируемой зоны. Съем осуществляется за счёт изменений параметров отражённого от предмета зеркально или диффузно зондирующего когерентного лазерного излучения (обычно в ближней ИК области). Такой ТКУИ носит название «вибрационный канал с применением аппаратуры дистанционного лазерного зондирования» или «электронно-оптический канал» (термин распространённый, но неверный, относящийся к совсем иному каналу утечки).

Акустоэлектрический канал. Прежде всего хотелось бы отметить, что в регламентирующих документах отсутствует понятие «каналы АЭП», или «акустоэлектрические каналы». Применяется термин «каналы утечки информации за счёт акустоэлектрических преобразований». Поэтому далее применение вышеупомянутого термина следует считать профессиональным сленгом. Акустоэлектрические каналы утечки информации возникают за счет преобразований акустических, а точнее — вибрационных, сигналов в электрические.

АЭП каналы подразделяется на два семейства подканалов, имеющие принципиальные отличия за счёт физической основы опасного сигнала:

- низкочастотные, «прямые» АЭП (НЧ АЭП);
- высокочастотные, модуляционные, параметрические АЭП (ВЧ АЭП).

В случае НЧ АЭП электрический сигнал, возникающий в элементах и/или цепях ВТСС, имеет тот же диапазон частот, что и воздействующий акустический сигнал, и пропорционален ему. Электрический сигнал звуковой частоты и весьма малой амплитуды (как правило, не

выше десятков милливольт) способен распространяться на заметные расстояния только по токопроводящим конструкциям.

В связи с этим предполагается, что приём (перехват) акустоэлектрических колебаний в данном канале утечки информации может быть осуществлён непосредственным подключением к соединительным линиям ВТСС специальных первичных преобразователей средства разведки. Например, подключая такие средства к соединительным линиям телефонных аппаратов, можно прослушивать разговоры, ведущиеся в помещениях, где установлены эти аппараты, при положенной на рычаги трубке.

Источники и механизмы возникновения этих опасных сигналов следующие. Многочисленные элементы ВТСС, в том числе различные моточные элементы, конденсаторы с сегнетодиэлектриками, ряд конструкций полупроводниковых компонентов и т. п., обладают свойством изменять свои параметры (емкость, индуктивность, магнитное и электрическое сопротивление, коэффициент передачи) под действием механического воздействия акустического поля, создаваемого источником речевого сигнала. Изменение параметров приводит либо к появлению на выводах элементах электродвижущей силы (ЭДС), либо к изменению протекающих токов в соответствии с изменениями воздействующего акустического поля.

ВТСС, кроме указанных элементов, могут содержать непосредственно специализированные электроакустические преобразователи. К таким элементам относятся пьезострикционные преобразователи, динамические головки прямого излучения, головные телефоны любых типов и т. д. Причем из элементов, обладающих микрофонным эффектом, наибольшую чувствительность к акустическому полю имеют абонентские громкоговорители, различные трансформаторы и электродвигатели, а также некоторые элементы датчиков пожарной и охранной сигнализаций.

Естественно, что этот же канал может и должен рассматриваться в отношении ТСПИ, хотя сам механизм образования электрических речевых сигналов в их цепях иной (не паразитный, а штатный), но методы измерения и нормированные параметры защищённости в отходящих линиях полностью совпадают.

Как и следует из физической природы носителя информации для данного канала, средой его распространения являются различные проводящие конструкции.

Высокочастотный канал АЭП возникает в соответствии с иным механизмом. Если в составе технического средства (ВТСС или ТСПИ) штатно присутствует генератор высокой частоты (неважно, синусоидальный или релаксационный) и в его цепях присутствует сигнал НЧ

АЭП или на его элементы воздействует акустический сигнал, то неизбежно возникает эффект модуляции ВЧ сигнала опасным речевым сигналом.

Механизм возникновения модуляции высокочастотной несущей низкочастотным сигналом на нелинейном элементе всесторонне разработан теоретической радиотехникой. Такой модулированный сигнал за счёт высокой частоты несущей способен не только распространяться по токопроводящим конструкциям, но и эффективно излучаться в пространство.

В отношении ТСПИ, в цепях которых циркулируют опасные сигналы значительных величин, этот вид ТКУИ особенно опасен, так как в этом случае следует ожидать весьма значительной степени модуляции несущих частот. Для ВТСС уровни модуляции, как правило, значительно меньше, но вполне достаточны для образования канала утечки.

Особенностью канала ВЧ АЭП является то, что весь объём информации может быть перехвачен при осуществлении радиоприёма и демодуляции как основной несущей частоты, так и любой из её, отдельно взятой, гармоники в достаточно узкой полосе частот — в соответствии с теорией $\Delta F \approx 2\Omega$ (где Ω — максимальная частота речевого сигнала ≈3,5 кГц). Таким образом, радиоканал перехвата является узкополосным и, следовательно, весьма помехозащищённым.

Среда распространения для канала НЧ АЭП — только проводящие конструкции, а для ВЧ АЭП ещё и свободное пространство.

Различны и параметры защищённости, методы измерений и расчётов для этих двух каналов.

Канал линейного ВЧ навязывания. Технический канал утечки информации с использованием высокочастотного навязывания реализуется контактным введением токов высокой частоты от соответствующего генератора средства разведки в линию, имеющую связи с нелинейными или параметрическими элементами ТСПИ или ВТСС, на которую одновременно воздействует акустический опасный сигнал.

При одновременном воздействии на эти элементы акустического сигнала (или сигнала НЧ АЭП) и зондирующего ВЧ сигнала возможна модуляция высокочастотного сигнала опасным сигналом. Рассматриваются как амплитудная, так и угловая (частотная и фазовая) модуляции. В ряде случаев модуляция может возникать и в линейных цепях, при этом она носит название параметрической модуляции. Промодулированный зондирующий сигнал будет распространяться в обратном направлении по линии или излучаться.

Наиболее часто такой канал используется для перехвата разговоров, ведущихся в помещении, через телефонный аппарат, имеющий выход за пределы контролируемой зоны.

Особенно опасным этот ТКУИ является для ТСПИ, поскольку в их цепях циркулируют речевые сигналы большой амплитуды и, следовательно, возможны большие значения модуляции зондирующего сигнала. Однако случай, когда ТСПИ, т. е. техническое средство, предназначенное для обработки закрытой информации, имеет отходящую линию, которая выходит за пределы КЗ (за исключением линии электропитания) является исключительным.

Как следует из названия данного канала, средой распространения его являются, преимущественно, различные проводящие конструкции.

Канал ВЧ облучения. Технический канал утечки информации, с использованием высокочастотного облучения, образуется за счет неконтактного (дистанционного, через свободное пространство) введения токов высокой частоты в ТС, имеющие нелинейные или параметрические элементы. Для этих целей используется соответствующий высокочастотный генератор средства разведки. Одновременно на эти элементы воздействует акустический опасный сигнал. При этом возможна модуляция зондирующего ВЧ сигнала акустическим опасным сигналом. Затем происходит обратное переизлучение зондирующего модулированного сигнала, его приём, демодуляция и, таким образом, перехват защищаемой речевой информации.

В результате воздействия акустического поля меняется давление на все элементы высокочастотных генераторов ТС, в том числе и линейные. При этом изменяется взаимное расположение элементов схем, проводов в катушках индуктивности, дросселей и т. п. Это может привести к изменениям параметров переизлучённого зондирующего высокочастотного сигнала, например к модуляции его информационным сигналом. Такой механизм модуляции носит название *параметрической модуляции*.

Как один из вариантов канала ВЧ облучения рассматривается облучение ТС электромагнитным полем мощных штатных источников, например ТВ и радиовещательных передатчиков. При проведении специальных исследований такие варианты ТКУИ регистрировались неоднократно.

Необходимо отметить, что полная модель каналов высокочастотного навязывания и модель каналов высокочастотного облучения может включать и комбинированные случаи, при которых рассматривается «подача» зондирующего сигнала по проводящей линии, а приём модулированного отражённого сигнала осуществляется «по эфиру». Аналогично должен анализироваться и обратный вариант.

Как и в случае высокочастотного навязывания, особенно опасным этот ТКУИ является для технических средств передачи информации, поскольку в их цепях циркулируют речевые сигналы большой

амплитуды и, следовательно, возможны бóльшие значения модуляции зондирующего сигнала.

Средой распространения данного канала является, преимущественно, свободное пространство.

Канал паразитной высокочастотной генерации (ПВЧГ). Данный технический канал утечки по своим физическим основам возникновения и распространения практически совпадает с каналом высокочастотных акустоэлектрических преобразований (ВЧ АЭП). Но в отличие от них, источником этой несущей частоты является не штатно функционирующий в составе технического средства генератор, а генератор паразитный, возникающий случайно в активных (усилительных) элементах технических средств за счёт паразитных обратных связей в некоторых режимах функционирования.

Особенно опасным этот ТКУИ является для технических средств передачи информации, поскольку в их цепях циркулируют речевые сигналы большой амплитуды и, следовательно, возможны бóльшие значения модуляции высокочастотных сигналов.

Учитывая нестабильность частоты, амплитуды и иных параметров таких генераторов, невозможность их сколько-нибудь надёжной оценки и регламентации, для этого ТКУИ не нормированы никакие параметры защищённости. Единственное принятое нормативное требование для этого канала — категорическое требование полного его отсутствия.

Как и следует из физической природы носителя информации для данного канала, средой распространения его является и, преимущественно, свободное пространство, и проводящие конструкции.

Канал ПЭМИН. Данный вид технического канала утечки, одноимённый каналу для ОТСС, имеет чётко выраженные особенности, позволяющие классифицировать его в отношении ТСПИ и ВТСС и связать с утечкой только речевой информации.

Как и следует из названия, это канал утечки через побочные электромагнитные излучения (поля). Источник этих полей и является ключевым понятием. Для ТСПИ, обрабатывающих только речевую информацию (по определению), — это цепи, узлы, блоки аппаратуры, в которых циркулирует речевая информация в аналоговой форме при достаточно большой амплитуде напряжения и/или токов. Например, линии «раздачи» мощности от усилителя к колонкам в системах озвучивания помещений или конференцсвязи, токи в динамических головках прямого излучения различных колонок (громкоговорителей), ряд других цепей. Когда токи достигают многих ампер, а напряжения сотен вольт, порождаемые ими поля могут быть перехвачены на расстояниях до сотен метров.

Но и при рассмотрении ВТСС не всё благополучно. Простой пример. В выделенном помещении находится музыкальный центр. Разумеется, он выключен (на время закрытого мероприятия). Схемотехника усилителя мощности предусматривает, что при выключении (обесточивании) усилителя мощности линии, ведущие к колонкам, закорачиваются (с целью защиты динамиков, их арретировании). Под воздействием речи в помещении диффузоры динамиков колеблются («обращённый», «микрофонный» режим динамика). При этом в звуковой катушке генерируется ЭДС со среднеквадратичным значением примерно 10...20 мВ. Сопротивление катушки 4 Ом, на конце линии — короткое замыкание. При этом в линии (3...5 м) протекает ток около 2,5...5 мА. В звуковой катушке примерно 40–60 витков, её диаметр около 4 см, длина 1 см.

Напряжённость поля в соленоиде конечной длины рассчитывается по формуле (учитывая низкие частоты можно применить формулы магнитостатики)

$$H = \frac{NI_{\text{с}}}{\sqrt{D^2 + L^2}} = 4{,}9 \text{ А/м},$$

где N — число витков соленоида; L — его длина; D — диаметр; $I_{\text{с}}$ — ток в соленоиде.

Конечно, поле вне соленоида быстро спадает, но и величина очень велика, такое поле вполне можно перехватить на расстоянии нескольких метров. Вот вам и канал утечки от обесточенного, неработающего устройства и одновременно классический случай ПЭМИН.

Всё вышеприведённое относится к сигналам в аналоговой форме, однако рассматривается и оцифрованная речевая информация. Необходимо отметить, что механизмы возникновения, измерения и оценки каналов утечки речевой информации за счёт ПЭМИН в такой форме очень близки к аналогичным методам для цифровой информации вообще, но есть отличия в подходах к образованию (и, соответственно, значениям) норм защищённости. Эти отличия связаны с самой природой речевого сигнала, его информативностью, избыточностью, разборчивостью.

Как и следует из физической природы носителя информации для данного канала, средой распространения его является свободное пространство.

1.2.3. Технические каналы утечки вибрационной информации (акустическая сигнальная разведка)

Некоторые технические средства передачи информации имеют в своем составе печатающие и другие механические и/или электромеханические устройства, для которых можно найти соответствие меж-

ду распечатываемым (набираемым) символом и его акустическим или вибрационным образом. Данный принцип лежит в основе канала утечки информации по вибрационному каналу.

Подробное рассмотрение данного канала выходит за рамки данного пособия.

1.2.4. Канал побочных электромагнитных излучений и наводок (разведка ПЭМИН)

Как следует из названия раздела, целью данного вида разведки является получение информации, содержащейся в побочных излучениях (электрических, магнитных и электромагнитных полях) технических средств, обрабатывающих, хранящих и передающих защищаемую информацию (ОТСС). Так как эти излучения не являются штатными, необходимыми для работы технического средства, они получили название побочных электромагнитных излучений. При распространении этих излучений в окружающей среде возможны наводки этих полей на любые токопроводящие конструкции (провода, кабели, металлические конструкционные элементы, системы электропитания, заземления и т. п.), следовательно, эти процессы также подлежат анализу и контролю.

Источниками ПЭМИН является широчайший спектр различных технических средств. Наиболее типичными представителями этих источников являются разнообразные средства вычислительной техники и другие технические средства, обработка (передача, хранение) защищаемой информации в которых, осуществляется в форме цифровых кодов.

Отличиями ПЭМИН сигналов ОТСС в цифровой форме от сигналов ПЭМИН технических средств передачи информации в аналоговой форме являются их принципиальная широкополосность и, как правило, совершенно различные частотные диапазоны. Минимальная ширина полосы приёма таких сигналов у средства разведки должна составлять единицы, а иногда и сотни МГц. Отсюда совершенно иные подходы к измерениям, расчётам и оценкам данного ТКУИ.

В ОТСС носителем информации является электрический ток, параметры которого (как правило, амплитуда) изменяются во времени в зависимости от конкретного метода кодирования. При прохождении изменяющегося электрического тока по токоведущим элементам ОТСС вокруг них возникают изменяющиеся электрические и магнитные поля. В силу этого элементы ОТСС, особенно соизмеримые с длиною волны колебания, можно рассматривать как излучатели электромагнитного поля (случайные антенны). Это поле переносит информацию о том, в какой момент и какие именно импульсы проходили по цепям (на основной частоте следования импульсов и её гар-

мониках), следовательно, возможен перехват этой информации, т. е. её утечка.

При нормировании параметра защищённости в этих каналах отношение сигнал/шум устанавливается для одного двоичного разряда. Соответственно, при рассмотрении информации, существующей в параллельных кодах (с разрядностью более 2), при проведении специальных исследований необходимо всю энергию сигнала пересчитывать на энергию одного разряда.

Как и следует из физической природы носителя информации для данного канала, средой распространения его являются, преимущественно, свободное пространство и, частично, токопроводящие коммуникации.

ПЭМИН на частотах работы ВЧ генераторов ОТСС. В состав ОТСС могут входить различного рода высокочастотные генераторы. К таким устройствам можно отнести в первую очередь задающие тактовые генераторы.

В принципе, можно допустить, что возможна модуляция, в том числе параметрическая, более высокочастотных «несущих» колебаний низкочастотными, несущими защищаемую информацию. Однако регламентирующие документы не рассматривают такой вариант. ПЭМИН именно тактовых генераторов рассматривается, и справедливо, как неинформативный, не несущий информации, имеющий фоновый, помеховый характер.

Как и следует из физической природы носителя информации для данного канала, средой распространения его является свободное пространство.

Варианты ТКУИ методами высокочастотного навязывания и высокочастотного облучения в отношении неречевой цифровой информации принципиально не отличаются от ранее рассмотренных и поэтому более подробно не рассматриваются.

Электрические каналы. Электрические каналы утечки информации возникают за счет:

- наводок электромагнитных излучений ОТСС на соединительные линии ВТСС и посторонние проводники, выходящие за пределы контролируемой зоны;
- просачивания информационных сигналов в отходящие от ОТСС линии, включая линии электропитания и цепи заземления.

Наводки электромагнитных излучений ОТСС на линии. Наводки возникают при излучении элементами ОТСС информативных сигналов, а также при наличии ёмкостных и/или индуктивных связей соединительных линий ОТСС и посторонних проводников или линий ВТСС.

Уровень наводимых сигналов в значительной степени зависит от мощности излучаемых сигналов, расстояния до проводников, а также длины совместного пробега соединительных линий ОТСС и посторонних проводников.

Случайной приёмной антенной является цепь ВТСС или посторонние проводники, способные принимать побочные электромагнитные излучения.

Случайные антенны могут быть сосредоточенными и распределенными. Сосредоточенная случайная антенна представляет собой компактное техническое средство (например, телефонный аппарат). К распределенным случайным антеннам относятся кабели, провода, металлические трубы и другие токопроводящие коммуникации.

Просачивание информационных сигналов в линии электропитания. «Просачивание» возможно при наличии магнитных или ёмкостных связей между информационными цепями ОТСС и входными цепями блока питания. Кроме того, токи усиливаемых информационных сигналов замыкаются через источник электропитания, создавая на его внутреннем сопротивлении дополнительное напряжение, которое может быть обнаружено в линии электропитания. Информационный сигнал может проникнуть в линию электропитания также в результате того, что среднее значение потребляемого тока в устройстве зависит от амплитуды информационного сигнала. Это создает неравномерную нагрузку на выпрямитель и приводит к изменению потребляемого тока по закону изменения информационного сигнала.

Просачивание информационных сигналов в цепи заземления. Кроме заземляющих проводников, служащих для непосредственного соединения ОТСС с контуром заземления, гальваническую связь с землей могут иметь различные проводники, выходящие за пределы контролируемой зоны. К ним относятся нулевой провод сети электропитания, экраны соединительных кабелей, металлические трубы систем отопления и водоснабжения, металлическая арматура железобетонных конструкций и т. д. Все эти проводники совместно с заземляющим устройством образуют разветвленную систему заземления, в которую могут просачиваться информационные сигналы.

Перехват информационных сигналов возможен непосредственным подключением к соединительным линиям ВТСС и посторонним проводникам, проходящим через помещения, где установлены ОТСС, а также к их системам электропитания и заземления.

Как и следует из физической природы носителя информации для данного канала, средой распространения его являются проводящие конструкции.

1.2.4. Технические каналы утечки видовой информации (оптико-электронная, визуальная оптическая, фотографическая разведка)

Наряду с информацией, присутствующей в речевой форме в помещениях и/или обрабатываемой в ТСПИ и ОТСС, важную роль играет *видовая информация,* получаемая техническими средствами перехвата в виде изображений объектов или документов.

Учитывая характер рассматриваемой нами информации (форму существования), можно выделить следующие способы ее получения:

- «наблюдение» носителей;
- съемка (снятие копий) носителей.

Наблюдение носителей. В зависимости от условий наблюдения и освещения для наблюдения за печатным документом или экраном монитора (проектора и т. д.) могут использоваться различные технические средства, такие как оптические приборы (монокуляры, подзорные трубы, бинокли, телескопы и т. д.), телевизионные камеры, для наблюдения в условиях пониженного освещения — приборы ночного видения, телевизионные камеры, тепловизоры.

Для наблюдения с большого расстояния используются средства с длиннофокусными оптическими системами, а при наблюдении с близкого расстояния — камуфлированные скрытно установленные телевизионные камеры. При этом изображение с телевизионных камер может передаваться как по кабелю, так и по радиоканалу.

Съемка носителей. Съемка носителей (текста, графики и т. д.) проводится для документирования результатов наблюдения и более подробного изучения объектов. Для съемки используются телевизионные и фотографические средства.

При съемке, так же как и при наблюдении, использование тех или иных технических средств обусловлено условиями съемки и временем суток. Для съемки днем или самосветящегося носителя (экрана) с большого расстояния используются фотоаппараты и телевизионные камеры с длиннофокусными объективами или совмещенные с телескопами.

Для съемки днем с близкого расстояния могут применяться портативные камуфлированные фотоаппараты и телекамеры, совмещенные с устройствами видеозаписи или передачи изображений по радиоканалу.

Съемка объектов в условиях низкой освещённости (несамосветящихся носителей) проводится, как правило, с близкого расстояния. Для этих целей используются портативные фотоаппараты и телевизионные камеры, совмещенные с приборами ночного видения, или тепловизоры, а также портативные закамуфлированные телевизионные

камеры высокой чувствительности, совмещенные с устройствами передачи информации по радиоканалу.

1.2.5. Несанкционированный доступ к информации, обрабатываемой средствами вычислительной техники

В общем случае программное обеспечение любой универсальной компьютерной системы состоит из трех основных компонентов: операционной системы, сетевого программного обеспечения (СПО) и системы управления базами данных (СУБД). Поэтому все попытки взлома защиты компьютерных систем можно разделить на три группы:

- атаки на уровне операционной системы;
- атаки на уровне сетевого программного обеспечения;
- атаки на уровне систем управления базами данных.

Атаки на уровне операционной системы. Защищать операционную систему, в отличие от системы управления базами данных, гораздо сложнее. Дело в том, что внутренняя структура современных операционных систем чрезвычайно сложна и поэтому соблюдение адекватной политики безопасности является значительно более трудной задачей.

Возможности НСД на практике в значительной степени зависят от архитектуры и конфигурации конкретной операционной системы. Однако имеются методы НСД, которые могут применяться практически к любым операционным системам:

- кража пароля (подглядывание за пользователем, когда тот вводит пароль);
- получение пароля из файла, в котором пароль был сохранен пользователем; кража внешнего носителя парольной информации и т. д.;
- сканирование жестких дисков компьютера;
- сборка «мусора» (если средства операционной системы позволяют восстанавливать ранее удаленные объекты);
- превышение полномочий (используются ошибки в программном обеспечении или в администрировании операционной системы);
- отказ в обслуживании (целью НСД является частичный или полный вывод из строя операционной системы).

Атаки на уровне сетевого программного обеспечения. Сетевое программное обеспечение является наиболее уязвимым, потому что канал связи, по которому передаются сообщения, чаще всего не защищен и всякий, кто может иметь доступ к этому каналу, соответственно может перехватывать сообщения и отправлять свои собственные. Поэтому на уровне сетевого программного обеспечения возможны следующие методы НСД:

- прослушивание сегмента локальной сети;
- перехват сообщений на маршрутизаторе;
- создание ложного маршрутизатора;
- навязывание сообщений (отправляя в сеть сообщения с ложным обратным сетевым адресом, злоумышленник переключает на свой компьютер уже установленные сетевые соединения и в результате получает права пользователей);
- отказ в обслуживании (при отправлении в сеть сообщения специального вида компьютерные системы, подключенные к сети, полностью или частично выходят из строя).

Для противодействия указанным методам НСД следует максимально защитить каналы связи и тем самым затруднить обмен информацией по сети для тех, кто не является легальным пользователем.

Атаки на уровне систем управления базами данных. Защита системы управления базами данных (СУБД) является одной из самых простых задач. Это связано с тем, что СУБД имеют строго определенную внутреннюю структуру и операции над элементами СУБД заданы довольно четко. В большинстве случаев несанкционированный доступ осуществляется преодолением защиты компьютерной системы на уровне операционной системы, что позволяет получить доступ к файлам системы управления базами данных с помощью средств операционной системы. Однако в случае, если используется СУБД, не имеющая достаточно надежных защитных механизмов, становится вполне вероятным преодоление защиты, реализуемой на уровне системы управления базами данных.

Программные закладки. Программная закладка — недокументированный модуль, внедряемый в общесистемные программные средства, прикладные программы и аппаратные средства информационных и телекоммуникационных систем.

Существуют три основные группы деструктивных действий, которые могут осуществляться программными закладками:

- копирование информации пользователя компьютерной системы (паролей, криптографических ключей, кодов доступа, конфиденциальных электронных документов), находящихся в оперативной или внешней памяти этой системы либо в памяти другой компьютерной системы, подключенной к ней через локальную или глобальную компьютерную сеть;
- изменение алгоритмов функционирования системных, прикладных и служебных программ;
- навязывание определенных режимов работы (например, блокирование записи на диск при удалении информации, при этом информация, которую требуется удалить, не уничтожается и может быть впоследствии скопирована).

1.3. Теоретические основы функционирования типовых технических каналов утечки информации

1.3.1. Основы теории электромагнитного поля

К электромагнитным каналам утечки информации относятся:

- излучение элементов средств вычислительной техники (СВТ);
- излучение на частотах высокочастотных генераторов СВТ, промодулированных информационными сигналами;
- излучение на частотах самовозбуждения узлов СВТ.

Остановимся более подробно на особенностях этого канала утечки информации для средств вычислительной техники (диапазон частот 10 кГц. . . 2 ГГц).

Основные закономерности и свойства электромагнитного поля описываются системой уравнения Максвелла:

$$\begin{aligned}
\operatorname{rot} \bar{H} &= \sigma \bar{E} + \varepsilon_0 \varepsilon_2 \frac{dE}{dt}; \\
\operatorname{rot} \bar{E} &= -\mu_0 \mu_2 \frac{dH}{dt}; \\
\operatorname{div} \bar{E} &= \frac{\rho}{\varepsilon \varepsilon_0},
\end{aligned}$$

где $\varepsilon_0 = 10^{-9}/(36\pi)$ Ф/м; $\mu_0 = 4\pi \cdot 10^{-7}$ Г/м.

Для гармонического сигнала, т. е.

$$\dot{E} = E\mathrm{e}^{i\omega t}; \quad \dot{H} = H\mathrm{e}^{i\omega t},$$

система уравнений Максвелла будет выглядеть как:

$$\begin{aligned}
\operatorname{rot} \dot{H} &= (\sigma + i\omega\varepsilon_0)\dot{E}; \\
\operatorname{rot} \dot{E} &= -i\omega\mu_0 H; \\
\operatorname{div} \dot{E} &= \frac{\rho}{\varepsilon_0}; \\
\operatorname{div} \dot{H} &= 0,
\end{aligned}$$

где $\operatorname{rot} E = \lim\limits_{\Delta S \to 0} \dfrac{1}{\Delta S} \oint\limits_S \bar{A}\, dl.$

Для решения приведенных уравнений Максвелла вводятся дополнительные параметры электромагнитного поля — электрический и магнитный запаздывающие потенциалы: φ и A:

$$\varphi = \frac{1}{4\pi\varepsilon_0 r} \int_v \rho \left(t - \frac{r}{i}\right) dv; \quad A = \frac{\mu}{4\pi r} \int_v \delta_i \left(t - \frac{r}{i}\right) dv,$$

где ρ и δ_i — объемные плоскости заряда и тока; r — расстояние до точки наблюдения.

Для линейного тока векторный потенциал

$$A = \frac{\mu_0}{4\pi r}\int_e \delta\, dl.$$

С учетом введенных параметров A и φ

$$\bar{E} = -\left(\operatorname{grad}\varphi + \frac{d\bar{A}}{dt}\right);$$

$$\bar{H} \equiv \frac{1}{\mu_0}\operatorname{rot}\bar{A},$$

где по определению

$$\operatorname{grad}\varphi = \left(\frac{d\varphi}{dx}, \frac{d\varphi}{dy}, \frac{d\varphi}{dz}\right).$$

Реальные излучатели СВТ можно рассматривать как совокупность элементарных электрических и магнитных излучателей (диполей).

Элементарный электрический излучатель (особенности электромагнитного поля в непосредственной близости от источника). В полярной системе координат элементарный электрический излучатель изображен на рис. 1.2.

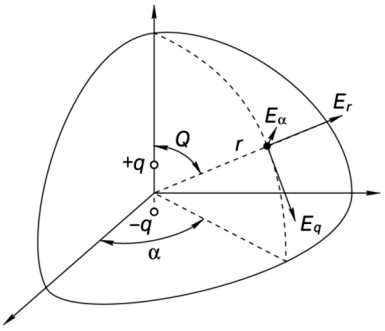


Рис. 1.2. Элементарный электрический излучатель

Компоненты электромагнитного поля элементарного электрического излучателя имеют следующий вид:

$$\dot{\bar{E}}_r = \frac{2\dot{J}l\cos\theta}{4\pi j\omega\varepsilon_0 r^3}(1 + j\alpha r^2)\mathrm{e}^{-j\alpha r};$$

$$\dot{\bar{E}}_\theta = \frac{\dot{J}l\sin\theta}{4\pi j\omega\varepsilon_0 r^3}(1 + j\alpha r - \alpha^2 r^2)\mathrm{e}^{-j\alpha r};$$

$$\dot{\bar{H}}_\alpha = \frac{\dot{J}l\sin\theta}{4\pi r^2}(1 - j\alpha r)\mathrm{e}^{-j\alpha r},$$

где $\alpha = 2\pi/\lambda = \omega/\mathrm{c}$; $\dot{J} = i\omega\dot{q}$.

В экваториальной плоскости (горизонтальная плоскость) имеем:

$$\dot{\bar{E}}_\theta = \dot{M}_\text{э}\left(\frac{1}{(\alpha r)^3} + \frac{j}{(\alpha r)^2} - \frac{1}{\alpha r}\right);$$

$$\dot{\bar{H}}_\alpha = \frac{\dot{M}_\text{э}}{\rho}\left[\frac{j}{(\alpha r)^2} - \frac{1}{\alpha r}\right],$$

где $M_\text{э} = \dfrac{ql}{4\pi\varepsilon\varepsilon_0}\alpha^3$ — параметр излучателя, в/м; $\rho = \sqrt{\dfrac{\mu_0}{\varepsilon_0}} = \dfrac{1}{\varepsilon_0 c}$;

$c = \dfrac{1}{\sqrt{\mu_0\varepsilon_0}}$ — скорость света в пустоте.

Первые два члена в выражении $\dot{\bar{E}}_\theta$ обусловлены $\operatorname{grad}\varphi$, а последний член — dA/dt. При $\alpha r < 1$ ($r \leqslant \lambda/2\pi$) ближняя зона излучения, напряженность электрического поля определяется как $\dot{E}_\theta =$ $= \dfrac{\dot{q}l}{4\pi\varepsilon_0}\dfrac{1}{r^3}$ — эта формула квазистатики, электрическое поле имеет потенциальный характер.

Для потенциального электрического поля

$$\oint E\,dl = 0 \quad (\operatorname{rot} E = 0).$$

Отношение

$$\frac{E_0}{H_\alpha} = \frac{1}{j\alpha r}\rho, \quad \rho = 377 \text{ Ом} = \sqrt{\frac{\mu_0}{\varepsilon_0}},$$

электрического поля высокоомное (десятки и сотни килоом), источники поля — открытые электрические заряды.

Учитывая, что соотношение компонент поля атмосферных помех $E_m/H_m = \rho$, R_2* определяется только электрическим полем E_θ.

В дальней зоне $\alpha r \gg 1$ (волновая зона)

$$|\dot{\bar{E}}_\theta| = \frac{M_э}{\alpha r} = \frac{ql\alpha^3}{4\pi\varepsilon\varepsilon_0}\frac{1}{\alpha r} = \frac{ql\alpha^2}{4\pi\varepsilon\varepsilon_0}\frac{1}{r}.$$

Отношение $E_\theta/H_\alpha = \rho = 377$Ом. Так как отношение компонент поля нормированных шумов в эфире $E_ш/H_ш = \rho = 377$ Ом, зона R_2 будет одинаковой как по магнитной, так и электрической составляющей.

На рис. 1.3 приводятся графики законов убывания компонент поля для элементарного электрического излучателя.

Решение уравнений Максвелла для элементарного магнитного излучателя. Компоненты электромагнитного поля элементарного магнитного излучателя имеют следующий вид:

$$\dot{\bar{H}}_2 = \frac{2JS\cos\theta}{4\pi\varepsilon^3}(1 + j\alpha r)\mathrm{e}^{-j\alpha r};$$

$$\dot{\bar{H}}_\theta = \frac{JS\sin\theta}{4\pi r^3}(1 + j\alpha r - \alpha^2 r^2)\mathrm{e}^{-j\alpha r};$$

$$\dot{\bar{E}}_\alpha = \frac{j\omega\mu_0 J\sin\theta}{4\pi r^2}(1 - j\alpha r)\mathrm{e}^{-j\alpha r}.$$

В полярной системе координат элементарный магнитный излучатель представлен на рис. 1.4.

---

* R_2 — расстояние между ОТСС и условной границей, за пределами которой невозможен эффективный прием вследствие естественного снижения уровня излучаемого сигнала, см. разд. 4.2. — *Прим. ред.*

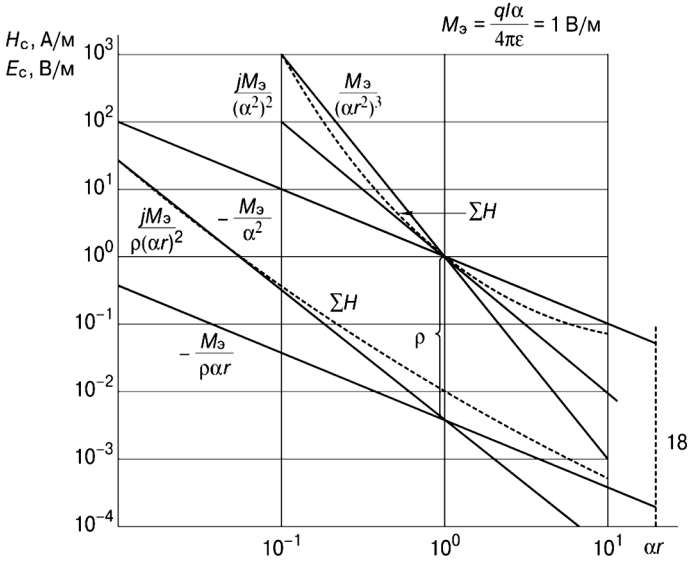


Рис. 1.3. Составляющие поля элементарного электрического излучателя

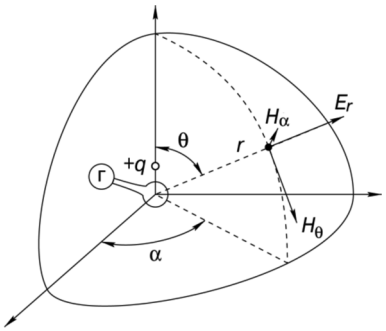


Рис. 1.4. Элементарный магнитный излучатель

Введем обозначения

$$\dot{M}_m = \frac{jS}{4\pi}\alpha^3; \quad \rho = \sqrt{\frac{\mu_0}{\varepsilon_0}} = \mu_0 C;$$

$$C = \frac{1}{\sqrt{\mu_0\varepsilon_0}}.$$

В экваториальной плоскости

$$\dot{\bar{H}}_\theta = M_m\left[\frac{1}{(\alpha r)^3} + \frac{j}{(\alpha r)^2} - \frac{1}{\alpha r}\right] \times$$

$$\times\, \mathrm{e}^{-j\alpha r};$$

$$\dot{\bar{E}}_\alpha = \rho M_m\left[\frac{j}{(\alpha r)^2} - \frac{1}{\alpha r}\right]\mathrm{e}^{-j\alpha r}.$$

Для ближней зоны $\alpha r < 1$ ($r < 0{,}16\lambda$)

$$\dot{\bar{H}}_\theta = \frac{JS}{4\pi r^3}$$

— это выражение магнитостатики.

Электрическое поле E_α незначительно и имеет вихревый характер (обусловлено членом уравнения dA/dt. Для него $\oint E\,dl \neq 0$.

Волновое сопротивление $E_\alpha/H_\theta = j\alpha r\rho$ — поле низкоомное (доли ома, либо единицы ом). Если считать, что $E_ш/H_ш = \rho$, то размер R_2 по H_θ будет намного больше, чем по E_α. Поле H_θ является оп-

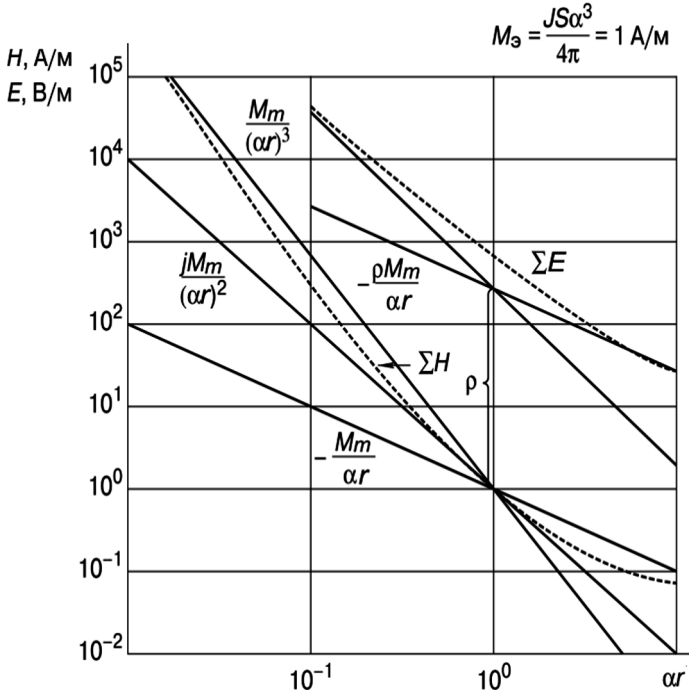


Рис. 1.5. Составляющие поля элементарного магнитного излучателя

ределяющим при оценке защищенности при расчете R_2. Для дальней зоны излучателя $\alpha r \gg 1$ $(r \geqslant 3\lambda)$

$$H_\theta = \frac{M_m}{\alpha r}; \quad \frac{E_\alpha}{H_\theta} = \rho.$$

Так как отношение компонент поля нормированных шумов в эфире $E_ш/H_ш = \rho =$ 377 Ом, зона R_2 будет одинаковой как по магнитной, так и электрической составляющей. На рис. 1.5 приводятся графики законов убывания компонент поля для элементарного магнитного излучателя.

Электрические излучатели электромагнитного поля. Физической моделью излучателя электрического поля СВТ для частот до 100 МГц является несимметричный излучатель с зарядом q. Этот переменный во времени заряд приподнят над проводящей поверхностью раздела электрических средств (в практике металлический каркас перекрытия пола, межэтажных перекрытий). Для решения задач вычисления электрического поля проводящая поверхность раздела электрических средств заменяется на зеркальное изображение этого заряда.

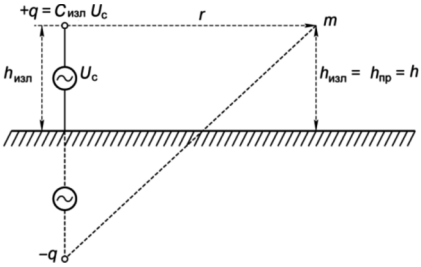


Рис. 1.6. Физическая модель излучателя электрического поля

Физическая модель излучателя электрического поля представлена на рис. 1.6. Для этой модели в ближней зоне излучателя

$$E = -\left(\operatorname{grad}\varphi + \frac{dA}{dt}\right);$$

$$\varphi_c = \frac{q}{4\pi\varepsilon_0}\left(\frac{1}{x} - \frac{1}{\sqrt{x^2+4}}\right),$$

где $x = r/h$.

Полный вектор электрического поля излучателя

$$E_c = \sqrt{E_{\text{вер}}^2 + E_{\text{гор}}^2},$$

где

$$E_{\text{вер}} = \frac{q}{4\pi\varepsilon_0 h^2}\frac{2}{(x^2+4)^{3/2}};$$

$$E_{\text{гор}} = \frac{q}{4\pi\varepsilon_0 h^2}\left[\frac{1}{x^2} - \frac{x^2}{(x^2+4)^{3/2}}\right].$$

Средневертикальная составляющая электрического поля СВТ (при измерении несимметричной электрической антенной)

$$E_{\text{св}} = \frac{\varphi_c}{h_{\text{пр}}} = \frac{q_{\text{изл}}}{4\pi\varepsilon_0 h^2}\left[\frac{1}{x} - \frac{1}{(x^2+4)^{1/2}}\right].$$

Для частот свыше 100 МГц физической моделью излучателя электрического поля ТС является элементарный электрический диполь.

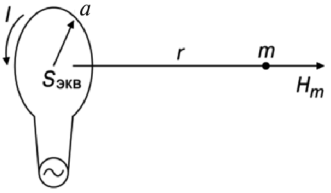


Рис. 1.7. Физическая модель излучателя магнитного поля

Магнитные излучатели электромагнитного поля. Физической моделью излучателя магнитного поля является рамка с площадью S, обтекаемой током I, изменяющимся по закону информационного сигнала (рис. 1.7).

Напряженность магнитного поля в непосредственной близости от излучателя определяется законами квазимагнитостатики.

В направлении оси рамки на расстоянии r направление максимального поля

$$H_m = \frac{Ia}{2(a^2+r^2)^{3/2}},$$

или

$$H_m = \frac{IS_{\text{экв}}}{2\pi(a^2 + r^2)^{3/2}},$$

где a — радиус излучающей рамки; r — расстояние до точки m.

При $r \gg a$, что обычно выполняется при пробных замерах поля при испытаниях ТС ($d = 1$ м)

$$H_m = \frac{IS_{\text{экв}}}{2\pi r^3},$$

т. е. магнитное поле убывает с расстоянием по закону $(1/r)^3$.

Вихревые составляющие электрического поля излучающей рамки в ближней зоне

$$E_{\text{вых}} = \alpha r \rho H = \alpha r \rho H_m/2.$$

Они не являются определяющими при расчёте радиуса зоны радиоперехвата.

Ввиду того, что при работе технических средств вычислительной техники возникают электрические и магнитные излучения, причем их соотношение между собой в общем виде неизвестно, необходимо измерять вблизи излучателя отдельно электрическое и магнитное поля (диполь, рамка) и отдельно рассчитывать R_2 по E и H и выбрать из них максимальное значение.

При измерении электрического поля (штыревая антенна или диполь) необходимо учитывать потенциальный характер электрического поля, исключать возможную ошибку за счет конечного значения затухания асимметрии согласующего устройства симметричной антенны (диполя).

1.3.2. Основы прикладной акустики

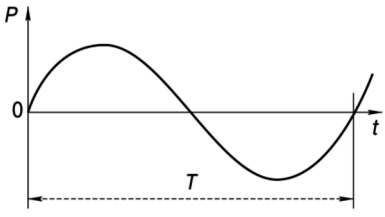


Рис. 1.8. Полный период колебания

Основные понятия, определения и единицы измерения в акустике. Звук — колебательное движение упругой среды. Процесс распространения колебательного движения в среде называется звуковой волной. За один полный период колебания T звуковой процесс распространяется в среде на расстояние, равное длине волны λ (рис. 1.8).

Длина волны зависит от скорости распространения звука в среде:

воздух ..... 340 м/с
вода ..... 1490 м/с
кирпич ..... 2300 м/с
бетон ..... 3700 м/с
сталь ..... 5200 м/с

Изменения давления в звуковой волне относительно среднего значения называется звуковым давлением P и измеряется в паскалях. Один паскаль — это давление, создаваемое силой в один ньютон, действующей на площадь один квадратный метр:

$$P = \frac{1\ \text{Н}}{1\ \text{м}^2} = 1\ \text{Па} = \frac{1}{100000}\ \text{атм}.$$

В акустике принято использование относительных единиц измерения уровня звукового давления — децибел:

$$L_{\text{дБ}} = 20 \lg \frac{P}{P_0}.$$

В качестве P_0 выбрано значение $P = P_0 = 2 \cdot 10^{-5}$ Па, что соответствует среднему минимальному звуковому давлению, воспринимаемому человеческим слухом. При этом изменение уровня звукового давления на 1 дБ является минимальным, различаемым человеческим слухом, изменением громкости.

Следует отметить, что в акустике при частотном анализе сигналов используют стандартизированные частотные полосы шириной в 1 октаву, 1/3 октавы, 1/12 октавы. Октава — это полоса частот, у которой верхняя граничная частота в два раза больше нижней граничной частоты:

$$\Delta f = (f_{\text{в}} - f_{\text{н}}) = 1\ \text{окт},$$

если $f_{\text{в}} = 2f_{\text{н}}$.

Среднегеометрические частоты стандартных октавных полос соответствуют следующему ряду: 2, 4, 8, 16, 31,5, 63, 125, 250, 500 Гц, 1, 2, 4, 8, 16 кГц.

Основные акустические параметры речевых сигналов. Основные звуки речи образуются следующим образом:

- гласные образуются при прохождении воздуха через голосовые связки. Акустические колебания гласных звуков носят периодический, близкий к гармоническому характер и могут изменяться в значительном частотном диапазоне;
- глухие согласные (сонорные, щелевые, взрывные) образуются за счет преодоления воздухом препятствий в носовой и ротовой полостях и носят характер как отдельных акустических импульсов, так и шумовых сигналов со сплошным спектром различной конфигурации;
- звонкие согласные образуются также как глухие, но при участии голосовых связок.

Таким образом, речевой сигнал представляет собой сложный частотно- и амплитудно-модулированный шумовой процесс, характеризу-

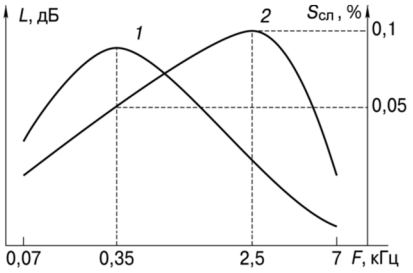


Рис. 1.9. Среднестатистический спектр русской речи

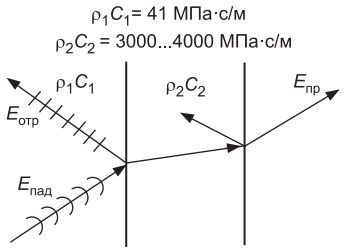


Рис. 1.10. Количество акустической энергии, прошедшей из одной среды в другую

ющийся следующими основными статистическими параметрами: частотный диапазон, уровень речевых сигналов, динамический диапазон.

Частотный диапазон речи лежит в пределах 70...7000 Гц. Энергия акустических колебаний в пределах указанного диапазона распределена неравномерно. На рис. 1.9 кривой *1* представлен вид среднестатистического спектра русской речи. Следует отметить, что порядка 95 % энергии речевого сигнала лежит в диапазоне 175...5600 Гц.

Важно отметить, что информативная насыщенность отдельных участков спектра речи неравномерна. Кривой *2* на рис. 1.9 представлен вклад отдельных участков спектра речи в суммарную разборчивость.

Уровни речевых сигналов. В различных условиях человек обменивается устной информацией с различным уровнем громкости, при этом создаются следующие уровни звукового давления:

тихий шепот ..... 35...40 дБ
спокойная беседа ..... 55...60 дБ
выступление в аудитории без средств звукоусиления .... 65...70 дБ

Динамический диапазон. Уровень речи в процессе озвучивания одного сообщения может меняться в значительных пределах. Разность между квазимаксимальными и квазиминимальными уровнями для различных видов речи составляет:

дикторская речь ..... 25...35 дБ
телефонные переговоры ..... 35...45 дБ
драматическая речь ..... 45...55 дБ.

Распространение акустических сигналов в помещениях и строительных конструкциях. При своем распространении звуковая волна, доходя до какой-либо преграды (границы двух сред, фазовый переход) и взаимодействуя с ней, частично отражается от нее, а частично продолжает распространяться внутри преграды. Количество акустической энергии, прошедшей из одной среды в другую, зависит от соотношения их акустических сопротивлений (рис. 1.10).

Таблица 1.1

Звукоизоляция основных строительных конструкций, дБ

Тип строительной конструкции	Центральные частоты октавных полос, Гц				
	250	500	1000	2000	4000
Оштукатуренная кирпичная стена толщиной 270 мм	44	51	58	64	65
Железобетонная стена толщиной 100 мм	40	44	50	55	60
Гипсобетонная перегородка толщиной 80 мм	33	37	39	44	44
Перегородка ДСП толщиной 20 мм	26	26	26	26	26

В строительной акустике используются следующие основные понятия:

- коэффициент поглощения $\alpha = (E_{\text{пад}} - E_{\text{отр}})/E_{\text{пад}}$;
- коэффициент отражения $\beta = E_{\text{отр}}/E_{\text{пад}}$;
- коэффициент звукопроницаемости $\gamma = E_{\text{пр}}/E_{\text{пад}}$;
- звукоизоляция $Q = 10\lg(E_{\text{пад}}/E_{\text{пр}})$.

Каналы утечки речевой информации. На рис. 1.11 представлены основные варианты возможной утечки речевой информации из объемов выделенных помещений. Все их можно объединить в две группы — это акустические каналы (обозначены буквами а, б, в), т. е. такие каналы, по которым информация может быть перехвачена с помощью микрофонов воздушной проводимости или прослушана непосредственно человеком, и вибрационные каналы (обозначены буквами г, д, е), т. е. каналы, по которым информация может быть зафиксирована с помощью микрофонов твердой среды (виброметров, велосиметров, акселерометров).

Наибольшую опасность представляют технологические окна и каналы с большой площадью поперечного сечения, такие как короба коммуникаций и воздуховоды вентиляции. Эти объекты являются, по сути, акустическими волноводами, и звуковые колебания могут распространяться по ним на значительные расстояния. Так, если поперечные размеры короба сравнимы с длиной звуковых волн $L \approx \lambda$, то затухание при распространении по нему звука $\delta = 0{,}01 \ldots 1$ дБ/м и зависит от размеров короба, материала стенок и пр.

Следующими по степени опасности являются звуководы с размерами значительно меньше длины звуковых волн $L \ll \lambda$. Таковыми могут быть отверстия электропроводки, щели и трещины в строительных конструкциях, неплотности дверных и оконных проемов. Затухание звука в таких каналах весьма значительно: $\delta = 1 \ldots 20$ дБ/м. Оно определяется вязкостью воздуха и зависит от поперечных размеров отверстий, шероховатости поверхности и продольной конфигурации отверстия.

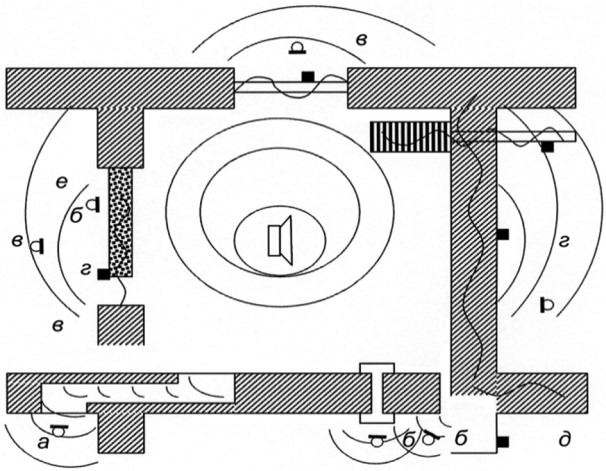


Рис. 1.11. Основные каналы утечки речевой информации

Несмотря на заметное затухание, этого абсолютно недостаточно для обеспечения защиты информации. Так, если в стене толщиной 0,5 м имеется трещина с площадью поперечного сечения 5 мм^2 и длиной 0,75 м, звукоизоляция в области выхода этой трещины на поверхность будет составлять 18 дБ, в то время как при отсутствии трещины такая стена может обеспечить звукоизоляцию более 65 дБ.

Звуковые колебания могут распространяться за пределы выделенного помещения не только за счет тех или иных воздушных каналов, но и за счет переизлучения колебаний ограждающими строительными конструкциями.

Переизлучение звука за пределы выделенного помещения происходит за счет колебаний строительных конструкций, вызванных падающими на них звуковыми волнами. Так как толщина подавляющего большинства строительных конструкций (стены, полы, потолки, двери, окна) значительно меньше их поперечных размеров, процессы, происходящие в них, хорошо описываются теорией колебания мембран и пластин.

Основные практические выводы, вытекающие из данных положений:

- акустическое сопротивление ограждающих строительных конструкций в направлении, перпендикулярном их поверхности, невелико;
- строительные конструкции имеют большое количество собственных мод колебаний.

Последнее явление в строительной акустике носит название «волнового совпадения». Оно возникает, когда длина падающей звуковой

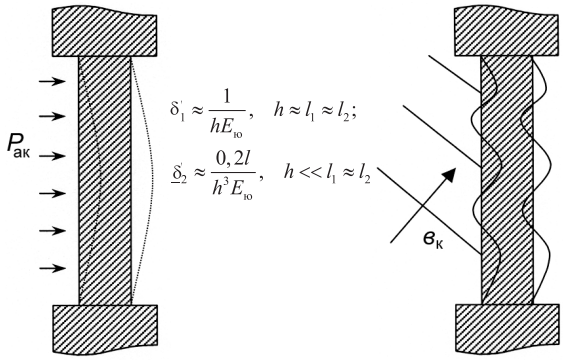


Рис. 1.12. Снижение звукоизоляции строительной конструкции

волны совпадает с длиной изгибной волны в строительной конструкции и приводит к значительному снижению звукоизоляции. Это проиллюстрировано на рис. 1.12.

Так как за счет многократных переотражений звуковой волны в помещении равновероятны любые углы падений, возбуждаются все собственные моды колебаний строительных конструкций, что приводит к существенному снижению звукоизоляции.

Вибрационные каналы. Как только что было показано, строительные конструкции совершают значительные колебания под воздействием акустических волн. Чтобы перехватить информацию, переносимую этими колебаниями, не обязательно регистрировать акустические колебания, переизлученные этими конструкциями, достаточно зафиксировать колебания собственно строительных конструкций. Так, например, под воздействием звука $P_{ак}$ = 70 дБ кирпичная стена толщиной 0,5 м совершает вибрационные колебания с ускорением $a \approx 3 \cdot 10^{-5}$ g. При таких условиях современными вибрационными датчиками может быть прослушан даже шепот. При этом переизлученный акустический сигнал будет $P_{ак.пр} < 10$ дБ,что практически исключает возможность съема информации. Таким образом, вибрационные колебания ограждающих конструкций под воздействием звуковых волн образуют один из наиболее опасных вибрационных каналов утечки информации.

Современные строительные материалы и конструкции (монолитный железобетон, сборные железобетонные конструкции, кирпичная кладка) обладают весьма низкими показателями затухания механических колебаний в области звуковых частот. Это обеспечивает возможность распространения колебаний на значительные расстояния и создает возможность перехвата информации, регистрируя вибрации не только ограждающих конструкций выделенного помещения, но и

регистрируя колебания значительно удаленных (1–3 стыка) элементов здания. Например, существует реальная возможность перехвата информации по несущей стене из выделенного помещения, расположенного через 1–2 этажа от места установки аппаратуры съема информации. В общем случае в зависимости от конструкции здания и качества выполнения стыков между его элементами затухание на стыках варьируется в пределах от 1...3 дБ до 10...15 дБ. Отсюда следует важная тактическая особенность и повышенная опасность вибрационного канала утечки информации — перехват информации возможен не только из смежных помещений, но и из помещений, значительно удаленных от источника информации.

Некоторые элементы строительных конструкций, как и в случае рассмотрения акустического канала, представляют собой волноводы вибрационных колебаний. К ним относятся трубы различных коммуникаций (отопления, водоснабжения, электропитания и пр.). Как и в случае воздушных волноводов, значительная разница в акустических сопротивлениях материала труб и окружающей среды составляет $(\rho C)_{\text{ст}}/(\rho C)_{\text{бет}} = 4...8$. Создаются условия волноводного распространения сигналов на значительные расстояния. Данный канал становится особенно опасным, если трубопровод соединен с какой-то жесткой и развитой поверхностью, которая играет роль согласующего элемента при передаче энергии из воздуха в трубопровод. Таким согласующим элементом, например, являются современные легкие, с большой площадью, радиаторы отопления.

Электроакустические преобразователи. Основным и обязательным элементом систем перехвата (и контроля) речевой информации, распространяющейся по акустическим и вибрационным каналам, является электроакустический преобразователь (акселерометр, велосиметр, тензометр). Электроакустический преобразователь является наиболее сложным физическим прибором в составе системы, определяющим как качество, так и тактические возможности применения системы в целом. Основной функцией электроакустического преобразователя является линейное преобразование акустической энергии в электрическую, с наименьшими потерями и искажениями. Процесс преобразования происходит в два этапа:

- преобразование энергии акустического (вибрационного) сигнала в упругие колебания механической системы преобразователя;
- преобразование колебаний механической системы в электрический сигнал.

Любое преобразование энергии из одного вида в другой связано с существенными потерями (кроме преобразования в тепло). Учитывая, что в электроакустических преобразователях осуществляется

двойное преобразование энергии, интенсивность акустического сигнала (при средней громкости речи) составляет 10^{-6} Вт/м^2 и площадь активной поверхности преобразователей составляет несколько квадратных сантиметров, становится очевидной сложность задачи создания высокочувствительного линейного широкополосного преобразователя.

Основными электроакустическими параметрами преобразователя являются:

- акустическая чувствительность, мВ/Па,

$$\gamma_a = \frac{U_{\text{эл}}}{P_{\text{ак}}},$$

где $U_{\text{эл}}$ — электрическое напряжение на выходе преобразователя; $P_{\text{ак}}$ — воздействующее на преобразователь акустическое давление;

- уровень собственного шума, дБ,

$$L_{\text{ш}} = 20 \lg \frac{U_{\text{ш}}}{\gamma_{\text{а}} P_0},$$

где $U_{\text{ш}}$ — электрическое напряженик собственных шумов; P_0 — «нулевой» уровень звукового давления, равный $2 \cdot 10^{-5}$ Па;

- вибрационная чувствительность, мВ/g,

$$\gamma_{\text{в}} = \frac{U_{\text{эл}}}{A},$$

где $U_{\text{эл}}$ — напряжение на выходе преобразователя; A — вибрационное ускорение, воздействующее на преобразователь, м/с^2;

- помехозащищенность, определяемая эквивалентным уровнем звукового давления и вибраций,

$$L_{\text{экв}} = 20 \lg \frac{\gamma_{\text{в}} g}{\gamma_{\text{а}} P_0}.$$

Факторы, влияющие на качество речевой информации, обеспечиваемое системой контроля (перехвата). Качество речевой информации (не путать со смысловым содержанием), получаемое от системы акустического контроля, принято оценивать разборчивостью, чаще всего словесной W или слоговой S. Качество принимаемой информации определяется как собственными параметрами аппаратуры перехвата, так и величиной и характером внешних воздействий. Разборчивость, в свою очередь, определяется отношением уровня информативного сигнала на выходе тракта передачи информации и суммарного уровня всех остальных сигналов, возникающих на входе и самом тракте передачи информации:

- уровень информативного сигнала

$$L_s = 20 \lg \frac{P_a \gamma_a k_u}{u_0};$$

- уровень вибрационных помех

$$L_{N_1} = 20 \lg \frac{A \gamma_в k_u}{u_0};$$

- уровень собственных электрических шумов

$$L_{N_2} = 20 \lg \frac{u_ш k_u}{u_0}.$$

Речевой сигнал, естественно, является основным фактором, определяющим качество получаемой информации. Считается, что минимальный уровень звукового давления членораздельной речи $L_{a\,\min} = 40$ дБ. Максимальный уровень звукового давления, развиваемого человеческим голосом, $L_{a\,\max} \approx 80$ дБ (по результатам оценки голосовых возможностей ведущих оперных певцов). Таким образом, динамический диапазон информативного речевого сигнала не превышает $\Delta L_a = 40$ дБ.

Частотный диапазон речевого сигнала лежит в пределах $f_н = 70$ Гц, $f_в = 7000$ Гц. Человеческая речь является весьма избыточным сигналом, поэтому для обеспечения минимально приемлемой разборчивости можно ограничить полосу сигнала частотами $f_н = 1400$ Гц, $f_в = 2900$ Гц, при этом слоговая разборчивость S будет составлять 30 %, а словесная W — 80 %. Следует отметить, что приведенные цифры справедливы в условиях отсутствия каких-либо мешающих факторов.

Воздействие помех требует существенного расширения частотной полосы речевого сигнала для сохранения той же разборчивости. Этим, собственно, и объясняется эволюционная целесообразность информационной избыточности речи (преимущественно выживали те группы людей, которые могли обмениваться речевой информацией в экстремальных условиях, связанных с сильными шумами: шум урагана, рев пламени, грохот падающей воды и т. п.).

Кроме обеспечения необходимой разборчивости речи, в условиях воздействия помех система перехвата речевой информации должна обеспечивать возможность идентификации личности говорящего человека. Для реализации этого требования необходимо регистрировать основание обертона и ближние гармоники голоса говорящего. Необходимые результаты в решении этих вопросов могут быть получены при расширении частотной полосы до $f_н = 250 \ldots 375$ Гц, $f_в = 4000 \ldots 6300$ Гц.

Основным фактором, ограничивающим качество информации, распространяющейся по акустическим и вибрационным каналам и принимаемой системой акустического контроля помещений, является воздействие акустических и вибрационных помех. Эти помехи могут быть как естественного (структурные шумы), так и искусственного (маскирующие помехи) происхождения.

Уровень структурных шумов индивидуален для каждого объекта контроля. Он зависит от структуры здания, его места расположения, насыщенности техническими средствами, количества людей и физической активности их деятельности, а также от погодных условий, времени суток и т. п.

Минимальный уровень структурных шумов, как правило, наблюдается в малоэтажных зданиях, выполненных из кирпича, или других мелкомасштабных строительных элементов и расположенных вдали от автомобильных и железных дорог, производственных и жилых зданий. Максимальные уровни строительного шума характерны для многоэтажных зданий из монолитного или сборного железобетона, расположенных рядом с интенсивными транспортными потоками или производственными предприятиями (цеха, производственные помещения и т. п. не рассматриваются).

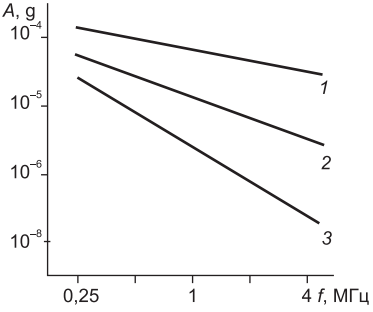


Рис. 1.13. Усредненные спектры естественных вибрационных шумов:
1 — $A_\Sigma = 3 \cdot 10^{-4}$ g, −3 дБ/окт;
2 — $A_\Sigma = 1 \cdot 10^{-4}$ g, −6 дБ/окт;
3 — $A_\Sigma = 3 \cdot 10^{-5}$ g, −9 дБ/окт

Статистическая обработка значительных массивов экспериментальных данных, полученных в результате измерений уровней структурных вибрационных шумов на различных действующих объектах, позволила выделить три основных типа вибрационной обстановки. На рис. 1.13 представлены усредненные спектры и суммарные значения ускорений вибраций в полосе частот $f_н = 250$ Гц, $f_в = 5000$ Гц, для шумной (*1*), средней (*2*) и тихой (*3*) вибрационной обстановки.

Следует заметить, что подавляющее большинство объектов акустической защиты относятся ко 2-му и 3-му типу вибрационной обстановки. Шумные вибрационные условия на реальных объектах встречаются крайне редко. Это объясняется тем, что объекты, представляющие существенный интерес для разведывательных служб, как правило, расположены в местах с достаточно комфортной акустической обстановкой.

Воздействие электронных шумов на качество речевой информации, принимаемой системой контроля, следует рассматривать с уче-

том взаимодействия электроакустического преобразователя и блока предварительной обработки информации.

В связи с широким разнообразием возможных типов электроакустических преобразователей и физических принципов их работы следует указать основные общие причины генерации напряжения электрических шумов. Это ограниченная электрическая и механическая добротность элементов механо-электрической системы преобразователя, которая, в свою очередь, определяется как собственными физическими параметрами применяемых материалов, так и совершенством технологии изготовления устройства в целом. Так, например, напряжение собственных электрических шумов в речевом диапазоне частот, наиболее распространенных в системах перехвата информации пьезокерамических преобразователей, $U_{\text{ш}} = 0{,}1 \ldots 0{,}3$ мВ.

Напряжение собственных шумов блока предварительной обработки информации, приведенные к его входу, нагруженному на эквивалент, соответствующий импедансу преобразователя, $U_{\text{ш}} = 0{,}2 \ldots 0{,}5$ мВ. Таким образом, суммарное напряжение собственных шумов, приведенное к входу системы преобразователь — блок предварительной обработки, не превышает (для пьезокерамических преобразователей) $U_{\text{ш}} = 0{,}6$ мВ и определяется, в основном, электронными шумами входных цепей блока предварительной обработки.

1.3.3. Основы процессов модуляции и возникновения ПВЧГ

Модуляция. Для понимания физических процессов, приводящих к образованию канала утечки информации за счет модуляции колебаний автогенераторов сигналами акустоэлектрических преобразований, рассмотрим простейшую схему LC-автогенератора с включенным LC-контуром в цепи положительной обратной связи (ПОС).

На самом деле различных схем генераторов достаточно много, но практически все они, как гармонические, так и релаксационные, строятся с применением в цепи ПОС либо LC-контура с полным или неполным включением реактивного элемента (индуктивности или емкости), либо фазосдвигающих RC-цепей (рис. 1.14).

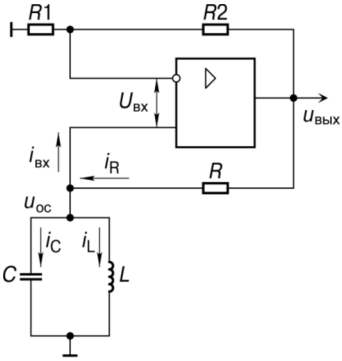


Рис. 1.14. Схема генератора

Генераторы с неполным включением реактивности на вход усилительного элемента получили название «трехточки». Независимо от схем автогенераторов, применяемых в конкретных тех-

нических средствах, все рассуждения об образовании данного канала утечки остаются действующими.

Физические принципы образования электрического сигнала под воздействием акустического сигнала рассмотрены выше. Однако стоит отметить, что для ВЧ генераторов даже незначительное отклонение значений реактивных элементов от номинала приводит к значительному изменению его параметров. Покажем это на примере приведенной выше схемы автогенератора.

Из курса радиотехники известно, что фазовая характеристика параллельного колебательного контура вблизи резонансной частоты определяется формулой

$$\varphi_{\text{к}} = \operatorname{arctg}(2Q\Delta f/f_{\text{р}}),$$

где $\Delta f = f - f_{\text{р}}$ — относительная расстройка колебательного контура; $f_{\text{р}}$ — резонансная частота контура. Тогда

$$\Delta f = f_{\text{р}} \operatorname{tg} \varphi_{\text{к}}/2Q.$$

Определим значение расстройки для следующих параметров контура: L = 160 мкГн; C = 160 пФ; Q = 50. Предположим, что на данный генератор действует гармонический акустический сигнал, под воздействием которого суммарный фазовый сдвиг $\varphi_{\text{к}}$ за счет всех дестабилизирующих факторов (изменения емкости и индуктивности, емкости монтажа и каких-то иных факторов, в данном случае это не принципиально) составил $\varphi_{\text{к}} = 25°$. В этом случае значение расстройки Δf составит 4500 Гц.

Несколько усложним приведенный пример, предполагая, что на автогенератор воздействует одновременно сложное колебание, представляющее сумму гармонических колебаний, каждое из которых в отдельности приводит к изменению тех или иных параметров контура, пусть даже в разной степени. В этом случае можно считать, что $\varphi_{\text{к}}$ является некоторой функцией от частоты воздействующего акустического сигнала $\boldsymbol{\Omega}$, а следовательно, $\varphi_{\text{к}} = \psi(\boldsymbol{\Omega})$ расстройки колебательного контура Δf, и частота выходного сигнала автогенератора также будут являться функциями от $\boldsymbol{\Omega}$, т. е.

$$\Delta f = \zeta(\boldsymbol{\Omega}); \quad F_{\text{ген}} = \gamma(\boldsymbol{\Omega}).$$

Но ведь с некоторым приближением и речевой сигнал может быть представлен суммой ортогональных составляющих, т. е. при акустическом воздействии речевого сигнала на автогенератор возможна модуляция его колебаний речевым сигналом.

Рассуждая подобным образом, несложно определить и логическую цепочку модуляции колебаний релаксационных автогенераторов воздействующим на них сигналом АЭП.

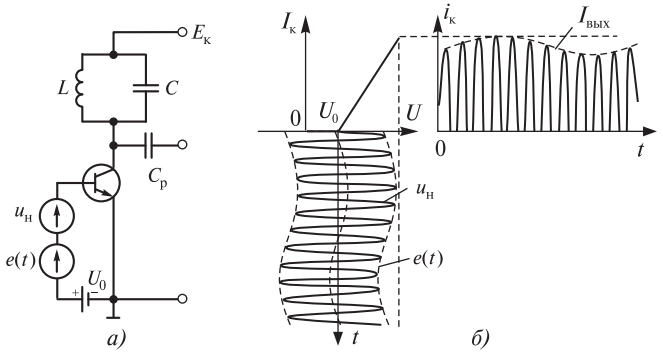


Рис. 1.15. Схема модулятора (*а*) и эпюры входного напряжения и выходного тока (*б*)

Кроме рассмотренного примера модуляции колебаний ВЧ автогенераторов при проведении специальных исследований нельзя забывать и об еще одном (хотя и очень распространенном) физическом принципе, приводящем к «паразитной» модуляции. Речь идет о нелинейном усилении сигналов. В интересующем нас случае рассматриваются усилители высокочастотных сигналов различного рода, выполняющих достаточно разные функции. Можно утверждать, что практически всякий усилитель является в определенной степени (вопрос только в большей или меньшей) нелинейным. На нелинейном усилении построена вся теория модуляторов, хорошо проработанная в теоретической радиотехнике.

Типовая упрощенная схема транзисторного амплитудного модулятора и поясняющие его работу диаграммы получения однотонального амплитудно модулированного сигнала приведена на рис. 1.15.

Для упрощения рассуждений сквозная характеристика транзистора — зависимость тока коллектора $I_к$ от напряжения база-эмиттер $U_{бэ}$ на диаграмме аппроксимирована двумя отрезками прямых линий. Вследствие перемещения рабочей точки относительно U_0 по закону низкочастотного сигнала $e(t)$ происходит изменение угла отсечки.

В результате импульсы коллекторного тока $i_к$ окажутся промодулированными по амплитуде, а выделенное резонансным контуром выходное напряжение также оказывается промодулированным. Не останавливаясь на параметрах элементов, влияющих на качество работы модулятора, отметим только, что для многотональной амплитудной модуляции (реальные сигналы) все приведенные здесь рассуждения полностью справедливы.

Паразитное возбуждение. Нередки случаи возникновения ПВЧГ в усилительных устройствах, выполненных с применением транзисторов и с достаточно низкой граничной частотой (чаще всего в блоках пита-

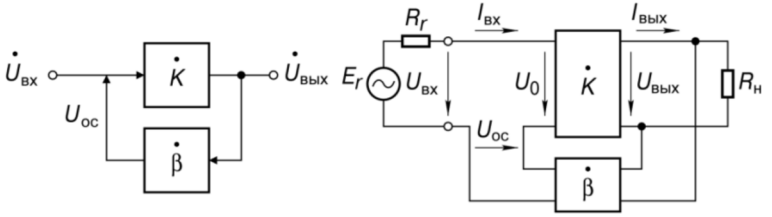


Рис. 1.16. Функциональная схема усилителя с ОС

ния различных технических средств) далеко за пределами $f_{гр}$. Объяснение этому явлению достаточно простое. С одной стороны, разработчики радиотехнических устройств при разработке схемотехники, как правило, выбирают транзисторы с $f_{гр}$ как минимум на порядок выше, чем максимальная частота усиливаемых сигналов. С другой стороны, «поведение» частотной характеристики за пределами $f_{гр}$ паспортными данными на транзисторы не нормируется. Достаточно часто встречаются случаи (и это подтверждено многочисленными экспериментами), когда АЧХ коэффициента усиления транзистора за пределами граничной частоты имеет резкий подъем ($K_{ус} \gg 1$), т. е. транзистор снова начинает усиливать.

Типовая схема усилителя с ОС приведена на рис. 1.16. В приведенной схеме $U_{вх}$ — напряжение на входе собственно усилителя; $U_{ос}$ — напряжение обратной связи; $K = U_{вых}/U_{о}$ — коэффициент усиления собственно усилителя (без ОС); $\beta = U_{ос}/U_{вых}$ — коэффициент передачи петли обратной связи.

В теории усилительных устройств коэффициент усиления усилителя с обратной связью принято определять как

$$K_{ос} = K/(1 - K\beta),$$

а параметр $K\beta = U_{ос}/U_{о}$ — как фактор обратной связи, или коэффициент усиления разомкнутого кольца обратной связи. Величина $(1 - K\beta)$ носит название глубины обратной связи.

Как следует из последней формулы, при значениях $0 < K\beta < 1$ коэффициент усиления усилителя с обратной связью $K_{ос}$ становится больше коэффициента усиления собственно усилителя K. Это соответствует положительной обратной связи (ПОС), при которой напряжение обратной связи $U_{ос}$ поступает на вход усилителя в фазе с входным $U_{вх}$, вследствие чего

$$U_{о} = U_{вх} + U_{ос}.$$

Значение $K\beta = 1$ характеризует условие самовозбуждение усилителя, когда он превращается в автогенератор широкого спектра частот, независимо от частоты входного сигнала.

Когда напряжение обратной связи находится в противофазе с входным, последняя формула перепишется следующим образом:

$$U_{\text{о}} = U_{\text{вх}} - U_{\text{ос}}.$$

В этом случае нетрудно показать, что

$$K_{\text{ос}} = K/(1 + K\beta),$$

т. е. коэффициент усиления усилителя уменьшится в $1 + K\beta$ раз. Такая обратная связь в усилителях называется отрицательной.

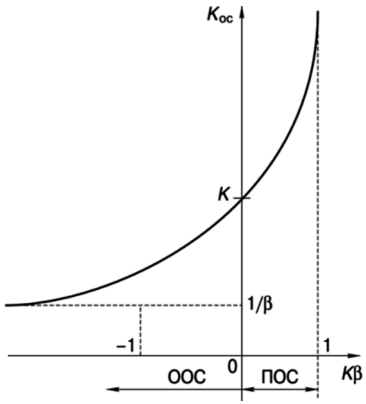


Рис. 1.17. Влияние обратной связи на коэффициент усиления усилителя

Наиболее наглядно влияние обратной связи на коэффициент усиления усилителя с обратной связью иллюстрируется с помощью графика (рис. 1.17), на котором можно выделить три характерные области:

- $K_\beta = 0$, так как $K \neq 0$, то $\beta = 0$ и коэффициент усиления усилителя равен K;
- $K\beta \to 1$ $K_{\text{ос}} \to \infty$. Физически бесконечно большой коэффициент усиления означает, что усилитель превращается в автогенератор электрических колебаний;
- $K\beta < 0$, что соответствует отрицательной ОС, частным случаем которой является 100%-ная ОС, при которой $K_{\text{ос}} = 1/\beta$ и не зависит от усиления собственно усилителя.

Практические схемы усилителей с обратной связью всегда содержат реактивные элементы, накапливающие энергию. Как уже говорилось выше, это могут быть межэлектродные емкости транзисторов и микросхем, паразитные емкости монтажа, индуктивности печатных проводников и монтажных проводов и т. д.

Реактивные элементы создают дополнительные фазовые сдвиги усиливаемых сигналов. Если на какой-то частоте сумма этих фазовых сдвигов достигает 180°, то обратная связьиз отрицательной переходит в положительную, превращая усилитель в автогенератор. В этом случае говорят о неустойчивости усилителя. Именно такой режим характеризует появление паразитной ВЧ генерации. В частном случае изменение параметров усилителей может быть вызвано воздействием акустических сигналов на элементы исследуемых ТС, о чем говорилось в разделе по модуляции.

В теоретической радиотехнике разработано много критериев определения устойчивости усилителей, наибольшее распространение из которых получил частотный критерий, или критерий Найквиста, при котором исследуется комплексный частотный коэффициент передачи

усилителя с разомкнутым кольцом обратной связи так называемой амплитудно-фазовой характеристики (АФХ). По определенной методике с помощью АФХ определяют устойчивость усилителя.

При этом понятно, что такая методика определения устойчивости приемлема только для относительно типовых и простейших усилительных каскадов и то только при их разработке. Расчет всего многообразия усилителей, входящих в состав даже одного технического средства, представляет собой неразрешимую задачу и в практике специальных исследований не используется.

Так как определить устойчивость любого усилителя для однозначного ответа об отсутствии ПВЧГ расчетным или каким-либо другим способом невозможно, приходится выполнять достаточно большой объем измерений при проведении СИ. Измерения приходится проводить во всех мыслимых и немыслимых режимах.

1.4. Закладочные устройства и защита информации от них

1.4.1. Построение и общие характеристики закладочных устройств

Радиоэлектронные закладочные устройства представляют собой организованный канал несанкционированного получения и передачи в пункт приема аудиовизуальной или обрабатываемой с помощью радиоэлектронной аппаратуры и передаваемой информации в сетях связи.

Закладочные устройства (ЗУ) можно классифицировать по нескольким признакам:

- радиозакладочные устройства, излучающие в эфир;
- закладочные устройства, не излучающие в эфир (с передачей перехваченной информации по сетям связи, управления, питания и т. д.);
- радиозакладочные устройства с переизлучением;
- закладочные устройства с передачей перехваченной информации по стандартному телефонному каналу.

В первую группу входят радиозакладочные устройства, предназначенные для получения аудиоинформации по акустике помещения, телевизионные закладочные устройства, ЗУ, предназначенные для получения аудио- и визуальной информации, радиозакладочные устройства в телефонных линиях связи, устройствах обработки и передачи информации, сетях питания и управления. Передача перехваченной информации происходит радио- или телевизионным радиосигналом.

К закладочным устройствам с передачей информации без излучения в эфир можно отнести группу закладочных устройств в линиях

связи, питания, управления и охранной сигнализации с использованием этих линий связи для передачи перехваченной информации.

В ряде закладочных устройств передача перехваченной информации осуществляется по стандартному телефонному каналу. Это так называемые закладки типа «длинное ухо», «с искусственно поднятой трубкой».

Существует целая группа закладочных устройств, обеспечивающих получение информации по акустике помещения за счет модуляции акустическим сигналом отраженного микроволнового или ИК сигналов от элементов, на которые воздействует акустический сигнал. Это могут быть стекла, окна, различные перегородки, резонаторы, специальные схемы и т. д.

Проявление рассмотренных выше групп закладочных устройств при передаче ими перехваченной информации различно, так как они могут проявляться в радиодиапазоне в виде радиоизлучений с различными видами модуляции или кодирования; в ИК диапазоне как низкочастотные излучения в линиях связи, управления, питания, в стандартных телефонных каналах или в виде облучающих сигналов.

В зависимости от предназначения закладочных устройств выделяется, прежде всего, зона несанкционированного получения информации. Это может быть воздушное пространство (для воздушной акустической волны), несущие конструкции, трубы водопроводной или паровой сети для структурной акустической волны, элементы тракта обработки и передачи информации и т. п.

Общие характеристики закладочных устройств

Исполнение: в виде отдельных технических модулей, технических модулей закамуфлированных под технические элементы и устройства, элементы одежды, бытовые предметы.

Мощность излучения:

- до 10 мВт — малая;
- от 10 до 100 мВт — средняя;
- более 100 мВт — большая;
- с регулируемой мощностью излучения.

Используемый вид модуляции:

- AM, FM, TNFM, WFM;
- частотноя мозаика;
- инверсия спектра;
- дельта-модуляция (адаптивная дельта-модуляция);
- шумоподобные сигналы;
- сигналы с псевдослучайным изменением частоты.

По стабилизации частоты:

- нестабилизированные;
- со схемотехнической стабилизацией частоты;

- с кварцевой стабилизацией.

Один из ограничивающих моментов использования закладочных устройств — гарантированная дальность перехвата информации. Эта дальность в ряде случаев является определяющей в организации поиска закладочных устройств. Применительно к закладочным устройствам, обеспечивающим перехват аудиоинформации, важна максимальная дальность перехвата либо воздушной, либо структурной волны датчиками съема подобной информации. В качестве таких датчиков используются микрофоны, стетоскопы или геофоны. Возможная дальность перехвата аудиоинформации, разговоров, передаваемых воздушной волной в пределах 10 м, структурной волной — через кирпичные и бетонные стены — 0,8...1,0 м и сейсмической волны — до 10 м при малых акустических шумах (до 5 м при средних акустических шумах).

Установка закладочных устройств перехвата информации из каналов обработки информации или систем передачи данных и связи определяется либо местом установки комплекса, либо возможностью установки закладочного устройства на линии связи.

Например, радиозакладочное устройство для перехвата телефонных переговоров может быть установлено в телефонной трубке, телефонном аппарате, соединительной коробке, разделительной телефонной коробке, на отрезках линий, соединяющих эти устройства, и т. д., вплоть до АТС. Место установки комбинированной телефонной закладки (перехват телефонных переговоров и акустики помещения) определяется зоной гарантированного перехвата акустической информации из определенного помещения (как правило, порядка 10 м от интересующего источника).

1.4.2. Радиозакладочные устройства

Перехваченная информация может быть передана по воздуху, по сетям питания, управления, связи для чего используются различного вида закладочные устройства.

Для выявления излучающих в эфир радиозакладок необходимо определить возможный диапазон их работы и используемые виды модуляции и закрытия. Анализ существующих радиозакладочных устройств позволил сделать вывод, что диапазон их работы достаточно широк и имеет тенденцию к продвижению в более высокие диапазоны, к использованию устройств с «прыгающими» частотами.

Основные диапазоны (по количеству известных образцов): 270... 480 МГц, 115...200 МГц, 75...115 МГц.

В последнее время увеличилось количество радиозакладочных устройств, работающих в диапазоне 640...1000 МГц и выше 1 ГГц. После введения ограничений на специальные технические средства

для радиозакладочных устройств выделен диапазон 415...450 МГц. Однако в эксплуатации можно встретить большое количество ранее выпущенных устройств. Таким образом, радиозакладочные устройства могут работать во всем диапазоне от 20 до 1000 МГц и выше.

Это существенно усложняет задачу поиска радиозакладочных устройств по их излучениям. Серьезное усложнение в поиске закладочных устройств вызывают изменяющиеся и совершенствующиеся виды модуляции и закрытия, используемые в современных закладочных устройствах. На начальном этапе радиозакладочные устройства строились с использованием амплитудной модуляции. Это позволяло использовать в качестве устройств перехвата излучаемой информации обычные бытовые приемники сответствующего диапазона. Однако это положительное качество часто превращалось в отрицательное, так как перехваченная и переданная в эфир информация легко обнаруживалась теми, кому она не предназначалась. Обыватели, прокручивая ручку своего бытового приемника, вдруг обнаруживали в эфире разговор своего соседа. Естественно, что такое обнаружение, как правило, приводило к последующему уничтожению иногда с очень большим трудом установленных закладочных устройств.

В радиозакладочных устройствах в основном применяется модуляция несущей частоты передатчика, однако встречаются радиозакладочные устройства с модуляцией сигнала промежуточной частоты или двойной модуляции (например, радиозакладка РК-1970-SS). Прием таких сигналов на обычный супергетеродинный приемник невозможен (после детектирования прослушивается обычный шум). Для приема может быть использован только специальный приемник.

В процессе появления и развития радиозакладок на нашем рынке существенное изменение претерпели и виды модуляции, используемой в них. И хотя все еще используются радиозакладки с WFM (широкополосной) и NFM (узкополосной) модуляцией, в наше время активно развивается принципиально новый класс радиозакладочных устройств с дельта-модуляцией. Кроме того, в профессиональных радиозакладках используют такие сложные сигналы, как шумоподобные или с псевдослучайной перестройкой несущей частоты. Например, в радиозакладках SIM-PR-9000T и РК-1970 используются шумоподобные сигналы с фазовой манипуляцией и шириной спектра 4 и 5 МГц.

При кодировании перехваченной информации часто применяется аналоговое скремблирование, изменяющее характеристики речевого сигнала таким образом, что он становится неразборчивым. Так, в радиозакладке РК-2010-S используется простая инверсия спектра с точкой инверсии 1,862 кГц, а в радиозакладке «Брусок-ЛЗБ ДУ», РК-1380-SS — сложная инверсия спектра. В ряде закладок используется преобразование речевой информации в цифровой вид (радиозакладки

PK-1195-SS, PK-2050), а в радиозакладках SIM-PR-9000T и PK-1970 наряду с преобразованием информации в цифровой вид используется ее шифрование [118].

В технических характеристиках ряда радиоприемных устройств поиска радиозакладок количество возможных для гарантированного перехвата видов модуляции и кодирования не перекрывает возможностей, заложенных в закладочных устройствах. Это существенно усложняет поиск закладочных устройств по их излучению, требует постоянной модернизации радиокомплексов для обеспечения поиска и перехвата, постоянно обновляемых и появляющихся новых видов модуляции и закрытия передаваемой перехваченной закладочными устройствами информации.

Существенное значение для организации каналов передачи перехваченной информации в радиодиапазоне имеет используемая в закладочном устройстве антенная система. В качестве таковой могут быть использованы собственное антенное устройство или случайная антенна.

В качестве *собственной антенны* обычно используется четвертьволновая антенна, имеющая круговую диаграмму направленности, что удобно для снимающего информацию, так как не предъявляет особых требований для установки аппаратуры перехвата, но размеры антенной системы зависят от используемого диапазона. В диапазонах ОВЧ и УВЧ в качестве антенны обычно используются проволочные четвертьволновые антенны, при переходе в СВЧ диапазон — штырьевая. Известны случаи использования в СВЧ диапазоне направленных антенных систем, что позволяет уменьшить риск обнаружения закладочного устройства, так как диаграмма направленности по максимуму в этом случае направлена на радиоприемное устройство съема информации. В качестве таких антенн часто используют спиральную или рамочную антенну.

Случайные антенны. Однако картина существенно изменяется, если в качестве передающей антенны используются отрезки линии передач, в которые включаются закладочные устройства, так называемые случайные антенны. Это может быть шнур, соединяющий трубку с телефонным аппаратом (в случае, если закладка помещена в телефонную трубку, например в капсулу телефонной трубки) или отрезки телефонной линии передачи (если закладочное устройство включается в розетку телефонной линии). В последнем случае длина этих отрезков может быть самой различной и диаграмма направленности и поляризационные характеристики антенны получаются самыми различными.

При использовании радиозакладок, работающих в ИК диапазоне, приемное устройство (с антенной) камуфлируется, как правило, в

приборах наблюдения или фотосъемки, так как для этого диапазона частот антенное устройство должно быть выполнено в виде фокусирующего устройства. Наряду с таким положительным качеством, как хорошее скрытие факта передачи, следует отметить необходимость строгой фиксации положения закладки и приемного устройства, а также обеспечение прямой видимости между ними (для обеспечения минимального затухания на трассе передачи перехваченной информации). Для противодействия перехвату излучений и выявлению радиозакладочных устройств в некоторых используется их включение только на момент проведения переговоров в том помещении, где радиозакладки установлены. Это может быть осуществлено включением в схему радиозакладки системы управления включения передатчика от голоса (система VAS или VOX). В этом случае радиозакладка работает (при отсутствии источника акустического сигнала) в режиме ожидания как приемник акустического сигнала и потребляет минимум энергии от источника питания. При появлении в помещении источника акустического сигнала система включает радиопередатчик и закладка работает в активном режиме с передачей перехваченного акустического сигнала. Включение такой системы в состав радиозакладки позволяет повысить ее скрытность и увеличивает время работы.

Для этих же целей может быть использована система дистанционного управления. Как правило, эта система используется для включения и выключения передатчика радиозакладки, а также для изменения режима работы передатчика, излучаемой мощности и параметров излучаемого сигнала.

Это довольно сложные системы, имеющие канал приема сигналов управления. В такой системе в дежурном режиме работает только радиоприемное устройство контроля управления, после подачи сигнала управления включается передающее устройство радиозакладки. Для передачи сигнала управления используется, как правило, УКВ диапазон, для избежания ложных срабатываний сигналы управления кодируются.

В настоящее время разработаны радиозакладочные устройства, которые могут контролировать несколько помещений (например, имеют два и более микрофона для контроля различных помещений). Система дистанционного управления позволяет осуществлять подключение контролируемых помещений, оптимизировать мощность излучения передатчика закладки в целях их защиты от перехвата радиоизлучений закладочного устройства.

Еще одним способом повышения скрытности передаваемой радиозакладкой информации является использование промежуточного накопления перехваченной информации. В состав такого устройства входит бескинематический цифровой накопитель, передатчик для

Рис. 1.18. Виды камуфлированных радиомикрофонов

ускоренной передачи накопленной информации и канал управления работой радиозакладки. В подобной радиозакладке в течение нескольких часов (6...14 ч) накапливается перехватываемая информация, а затем в течение 7...14 мин передается в эфир. Естественно, что использование возможных способов сокрытия передаваемой информации существенно сказывается на требованиях к радиоприемным устройствам поиска закладочных устройств по их излучению.

Конструктивно радиозакладочные устройства могут выполняться в виде технологических модулей или камуфлироваться в различные бытовые устройства.

На рис. 1.18 представлены камуфлированные радиомикрофоны. Для камуфляжа применяются различные бытовые, хозяйственные предметы или элементы радиоэлектронных устройств (картонка, корзина для мусора, конденсатор и т. п.).

Широкое применение нашли радиозакладочные устройства, закамуфлированные в бытовые предметы, сопутствующие разговаривающим собеседникам, — пепельницу, вазу, зажигалку, калькулятор. Часто для камуфляжа используют тройники, переходные устройства, настольные лампы, элементы одежды и т. п., располагающиеся в местах, где проводятся переговоры (рис. 1.19).

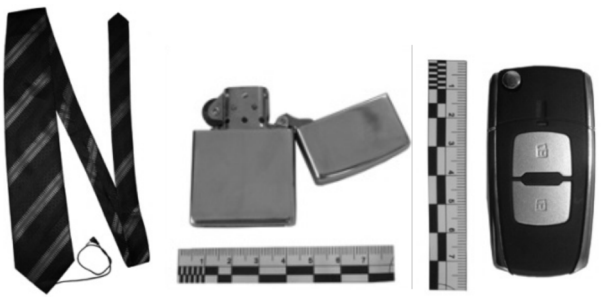


Рис. 1.19. Варианты закамуфлированных радиозакладок

Определенные ограничения на использование радиозакладочных устройств оказывают необходимые для их работы источники питания. Проблема не стоит остро, если для питания используются внешние источники питания — сеть питания (постоянная или переменная), телефонная линия связи, источники питания устройств, под которые закамуфлированы радиозакладочные устройства. Однако и при этом мощность, отбираемая из этих сетей для питания радиозакладок, должна быть ограниченной. Это связано, прежде всего, с тем, чтобы по отбору этой мощности нельзя было определить наличие закладочного устройства. Данное требование ограничивает мощность таких радиозакладок и дальность их действия. При питании радиозакладочных устройств от автономных источников питания (батарей, аккумуляторов и т. п.) время их работы может составлять от нескольких часов до нескольких месяцев. Использование схем управления работой передатчика (систем VAS, VOX, дистанционных систем управления работой передатчика и т. п.) позволяет увеличить временной интервал работоспособности радиозакладочного устройства и довести его до нескольких месяцев, а при обеспечении режима работы закладки по включению — до одного-двух месяцев.

Известны случаи, когда питание радиозакладочных устройств осуществлялось от систем светопреобразования, причем такие системы работают как от естественного, так и от искусственного света. Например, такой светопреобразователь может начинать работу при включении света в помещении, где установлена закладка, и, следовательно, такая радиозакладка будет работать только в момент наличия света в помещении.

1.4.3. Радиозакладочные переизлучающие устройства

Первые сведения о радиозакладочных устройствах с переизлучением относятся к середине 1940-х годов, когда в одном из патентов было описано устройство, в конструкцию которого был определенным образом включен четвертьволновый резонатор, настроенный на частоту 330 МГц (рис. 1.20).

Оболочка резонатора «прозрачна» для волн УКВ диапазона, и поэтому волна от внешнего источника этой частоты эффективно отражается от резонатора. С другой стороны, его расположение на слое маслянистой жидкости приводит к тому, что при возникновении акустического поля резонатор приходит вместе с этим слоем в микроколебания, соответствующие акустическому (речевому) сигналу, и в такт с этими колебаниями изменяются добротность и резонансная частота резонатора.

Отраженный сигнал, таким образом, модулируется информационным акустическим сигналом и в месте приема может быть довольно легко выделен. Спецслужба Великобритании (MI5) создала копию

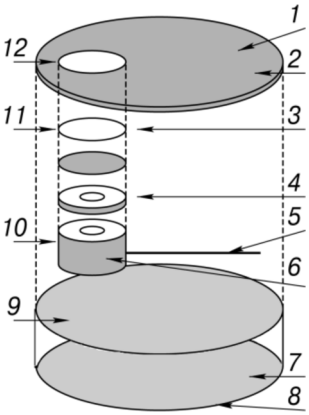


Рис. 1.20. Конструкция переизлучающей радиозакладки: *1* — крышка из диэлектрического материала; *2* — место стыковки с металлическим цилиндрическим стаканом; *3* — вставная крышка из ферритового материала; *4* — кольцо из изолятора; *5* — металлическая антенна (четвертьволновый вибратор на частоту 330 МГц); *6* — согласующий подстроечный конденсатор; *7* — специальная жидкость; *8* — стакан; *9* — тонкий слой маслянистой жидкости, реагирующей на звуковые колебания; *10* — металлический цилиндр, представляющий собой 1/2 катушки индуктивности на 10 мГн; *11* — металлический цилиндр; *12* — отверстие для установки резонатора с антенной

этого устройства, которое использовалось спецслужбами как Великобритании, так и Америки под кодовым названием «Сатир».

Принцип модуляции отраженного радиосигнала положен в основу действия специальных устройств, называемых аудиотранспондерами (от англ. audiotransponder) или эндовибраторами. Аудиотранспондеры состоят из переизлучающей антенны с резонансной системой, настроенной на частоту облучающего сигнала, приемника акустических колебаний и модулятора (рис. 1.21).

Параметры резонансной системы (резонансная частота или добротность) изменяются модулятором в соответствии с акустическим сигналом, принимаемым приемником акустических колебаний. Изменение параметров резонансной системы вызывает изменение отражающих свойств антенны, что приводит к модуляции отраженного радиосигнала.

Различают пассивные (не содержащие элементов питания и радиоэлектронных компонентов) и полуактивные аудиотранспондеры.

В пассивных аудиотранспондерах роль приемника акустических колебаний и модулятора выполняет подвижная диафрагма, а в качестве резонансной системы используются объемные резонаторы или резонансные линии. Пример пассивного аудиотранспондера на отрезке резонансной коаксиальной линии и его эквивалентная электрическая схема приведены на рис. 1.22.

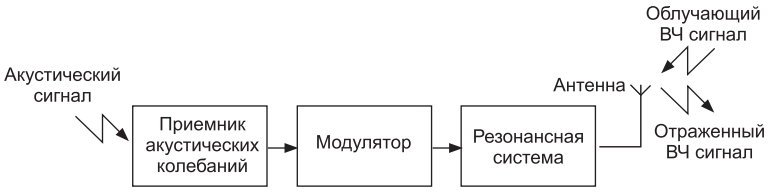


Рис. 1.21. Функциональная схема аудиотранспондера

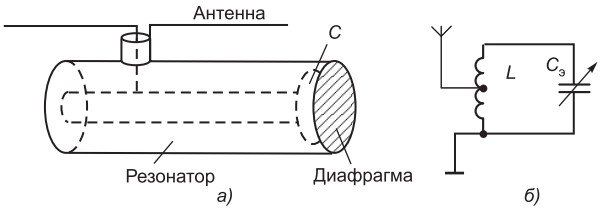


Рис. 1.22. Пассивный аудиотранспондер на коаксиальном резонаторе

Изменение отражающих свойств антенны, подключенной к резонатору, происходит за счет изменения резонансной частоты резонатора, вызванного перемещением диафрагмы и изменением емкости C под воздействием акустических колебаний. В качестве диафрагмы может использоваться тонкая металлическая мембрана или тонкий слой электропроводящей жидкости на дне резонатора. На эквивалентной электрической схеме (рис. 1.22,*б*) резонансный контур образован эквивалентной распределенной индуктивностью резонатора L и эквивалентной распределенной емкостью $C_э$, в которую входит переменная емкость C, образованная диафрагмой и центральным проводником коаксиальной линии. Резонансная частота такого резонатора определяется его геометрическими размерами, которые сравнимы с четвертью длины волны облучающего сигнала. В качестве антенны может использоваться полуволновый симметричный вибратор.

Основное достоинство пассивных эндовибраторов — отсутствие радиоэлектронных компонентов и элементов питания, что позволяет выполнять их в виде сувениров, предметов интерьера или элементов ограждающих конструкций, содержащих металлические элементы, геометрические размеры которых специально подобраны для образования эндовибраторного эффекта.

Недостаток пассивных эндовибраторов — малое изменение резонансной частоты или добротности резонатора, что ограничивает коэффициент модуляции отраженного сигнала и для обеспечения необходимой дальности перехвата акустической информации требует использования значительной облучающей мощности.

Полуактивные аудиотранспондеры позволяют получить больший коэффициент модуляции за счет изменения параметров резонансной системы электронным способом (например, с помощью варикапа). Упрощенная схема такого полуактивного эндовибратора приведена на рис. 1.23. Приемником акустических колебаний в этом случае является обыкновенный микрофон, а модулятором — усилитель звуковой частоты (УНЧ). Под

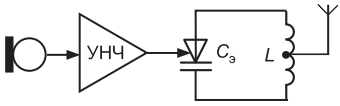


Рис. 1.23. Полуактивный аудиотранспондер

действием сигнала с выхода УНЧ изменяется резонансная частота колебательного контура LC.

Более сложные схемы полуактивных эндовибраторов позволяют помимо увеличения коэффициента модуляции усиливать отраженные высокочастотные колебания (ретрансляторы), изменять частоту несущей отраженного сигнала (конверторы), использовать другие более сложные виды модуляции (частотную, однополосную, цифровую и т. п.).

Полуактивные эндовибраторы имеют в своем составе электронные элементы, а следовательно, и демаскирующие факторы способствующие их обнаружению. По сути они представляют собой управляемые внешним сигналом устройства, передающие информацию по радиоканалу и при отсутствии облучающего сигнала могут быть выявлены по наличию нелинейных радиоэлектронных элементов. По сравнению с управляемыми радиозакладочными устройствами полуактивные эндовибраторы могут значительно дольше работать от автономного источника питания, так как потребляемая ими мощность не расходуется на излучение радиосигнала.

Примерами зарубежных аудиотранспондеров являются закладочные устройства (SIM-ATP-16, PK-500 и др.).

Подобные устройства работают в УКВ и СВЧ диапазонах. Передатчик узкополосным, практически моночастотным сигналом облучает транспондер, в приемнике которого выделяется зондирующий сигнал и подается на модулятор. В качестве модулирующего используется сигнал, поступающий с микрофона или микрофонного усилителя.

Промодулированный отраженный сигнал переизлучается на фоне более мощного облучающего сигнала (в целях его маскировки его частоту несколько сдвигают относительно частоты облучающего сигнала). Например, для аудиотранспондера SIM-ATP-16 резонансный контур выходного каскада транспондера расстроен относительно частоты облучающего сигнала на частоту 12 кГц (облучающий сигнал 160 МГц, переизлученный 160,012 МГц).

Приемопереизлучающая система использует плоскую кольцевую антенну. Транспондер имеет размеры 90×90×4 мм, что позволяет легко маскировать его в помещении. Мощность переизлученного сигнала зависит от мощности облучающего сигнала, и если последняя находится в пределах 10 Вт, то обеспечивается дальность перехвата 50...300 м.

Время функционирования транспортера 2000...4000 ч. Использование в качестве облучающей более высокой частоты позволяет уменьшить размеры аудиотранспондера. Так, в SIM-TP-40, где в качестве облучающей используется частота 800...950 МГц, размеры

транспондера 6×24 мм. При питании от внутренней батареи с напряжением 3В время работы транспондера около 4 месяцев.

1.4.4. Закладочные устройства типа «длинное ухо»

Отдельной, по принципу работы, является группа закладочных устройств, относящаяся к закладкам типа «длинное (телефонное) ухо» или закладка «с искусственно поднятой трубкой». Последнее название достаточно точно определяет принцип работы этого типа закладочного устройства.

При опущенной телефонной трубке на телефонную линию замкнута система вызова (механическая или электрическая), которую инициирует сигнал вызова. Когда абонент поднимает трубку, к линии подсоединяется телефонный аппарат и обеспечивается связь. Закладка с «искусственно поднятой трубкой» обеспечивает подсоединение телефонного аппарата и, следовательно, микрофона телефонной трубки (или дополнительного микрофона) к линии без механического подъема телефонной трубки.

Подача сигнала об искусственном подъеме телефонной трубки может осуществляться различными способами. Например:

- набирается номер телефона с закладкой;
- после первого (второго и т. п.) вызывного сигнала кладется трубка (при этом вызов в самом телефонном аппарате подавляется);
- через определенный интервал времени (10...40 с) осуществляется повторный вызов;
- для того чтобы посторонний, случайно попавший с вызовом в этот отрезок времени, не подключился к системе, через 45...60 с идет сигнал отбоя;
- через указанный промежуток времени закладочное устройство подключается к линии и идет контроль акустики помещения. Следует отметить, что при подключении к телефонному аппарату дополнительных микрофонов может быть организован контроль других помещений;
- при поднятии телефонной трубки закладка отключается.

Известны и другие способы подключения телефонов с закладкой:

- после набора номера телефона с закладкой в телефонную линию транслируется специальный звуковой сигнал через микрофон аппарата прослушивания (подобное устройство называется бипером);
- при прохождении этого специального сигнала система подключает телефон с закладкой на прослушивание.

Особенностью подобных закладочных устройств является их большая дальность действия — практически по всему земному шару.

1.4.5. Сетевые закладочные устройства

Электросеть здания и ее элементы могут быть использованы злоумышленником для установки и питания закладочных устройств, а также передачи перехваченной информации. Проводные системы скрытого аудиоконтроля предназначены для негласного съема и передачи аудиоинформации по проводным линиям. Прием сигналов аудиоинформации производится специальными приемниками серии КПЛ.

Изделия серии КПЛ предназначены для контроля акустической обстановки помещения с передачей информации по линиям проводных коммуникаций: электрической сети переменного тока — 220 В частотой 50 Гц (КПЛ-С) или телефонной сети на поднесущих частотах (КПЛ-Т). Прием передаваемой информации осуществляется на специальное приемное устройство, позволяющее принимать сигнал от трех передатчиков информации. Приемник оснащен гнездами для подключения головных телефонов, диктофона и внешнего источника питания. Кроме того, закладочные устройства могут быть закамуфлированы под розетку, тройник-розетку, различные переходники, в лампах, электрических светильниках, торшерах и т. п. Часть закладочных устройств выпускается без камуфляжа для того, чтобы потребитель мог их устанавливать по своему усмотрению.

Закладочные устройства, связанные с электросетью, могут быть условно разделены на две группы:

- закладочные устройства, обеспечивающие контроль акустической информации помещения с передачей перехваченной информации по сети электропитания;
- радиозакладочные устройства, обеспечивающие акустический контроль помещения с питанием от сети электропитания и передачей перехваченной информации по радиоканалу.

Одной из существенных особенностей подобных закладочных устройств является неограниченное время их работы (пока есть сеть питания). Закамуфлированные под широко используемые в быту и работе такие приборы, как удлинители, тройники, настольные лампы и другие бытовые электроприборы, подобные закладочные устройства довольно просто могут быть «внедрены» в интересующее помещение. В подобных устройствах акустический канал микрофона выполняется как конструктивные зазоры устройства, в которые камуфлируется закладка.

Габариты устройств камуфляжа обеспечивают расположение передающих устройств и при необходимости антенных систем.

Все устройства камуфляжа сохраняют свое прямое предназначение. Включение закладочных устройств обеспечивается, как правило, включением камуфлирующего устройства (удлинитель, тройник и т. п.) в сеть.

Однако для таких устройств существует ряд ограничений. Например, не рекомендуется использовать изделие для подключения приборов с большим потреблением электроэнергии (более 0,5 кВт), так как иначе может появиться сетевой фон в акустическом канале. Не рекомендуется устанавливать радиомикрофон вблизи источников акустических помех — холодильника, вентилятора, трансформатора, телевизора и т. п.

Для обеспечения большей скрытности закладочных устройств используется дистанционное управление, позволяющее включать закладное устройство только на необходимое время. Рассмотрим основные характеристики некоторых закладочных устройств с питанием от электросети и передачей информации по сети электропитания.

Сетевой микрофон «Сеть-IP» предназначен для длительной передачи речевой информации по имеющейся в здании электросети. Выполнен в виде стандартной электрической розетки. Дальность передачи информации не менее 100 м, питание от электрической сети, время работы не ограничено, прием ведется на специальный приемник.

Сетевой микрофон «Сеть-2НК» предназначен для контроля акустики в помещении и передачи полученной информации по сетям электропитания в ультразвуковом диапазоне частот. Прослушивание осуществляется на головные телефоны, имеется возможность подключения диктофона. Потребляемая мощность передатчика 100 мВт, частотная модуляция, несущая частота 100 кГц, время работы не ограничено, чувствительность приемника не менее 20 мкВ.

Комплект передачи информации по сети 220 В предназначен для контроля акустики в помещении и передачи информации по сети переменного тока 220 В, 50 Гц. Габаритные размеры 45×25×10 мм. Несущая частота 1,6...2,2 МГц, частотная модуляция, девиация сигнала 30...60 кГц, выходное напряжение 200...300 мВ, потребляемый от сети ток 5...15 мА; полоса передаваемого сигнала 0,3...6,0 кГц.

Система аудиоконтроля помещения по сети 220 В SEL-M220-01 состоит из передающего устройства SEL-M220-01 и приемника SEL-SP-35/CP. Предназначена для негласного получения акустической информации помещения и передачи ее по сети электропитания 220 В в пределах одной фазы. Диапазон частот 200...500 кГц, фазовая модуляция, дальность передачи до 100 м.

Система аудиоконтроля помещения по сети 220 В КПЛ-С предназначена для контроля акустики помещения с передачей информации по сети переменного тока 220 В 50 Гц. Габариты — 45×25×10 мм, питание от электросети 220 В частотой 50 Гц или встроенный аккумулятор. Передатчик информации с несущей частотой 1,6...2,2 МГц фазовой модуляции, полоса передаваемого сигнала 0,3...6,0 кГц. При-

Рис. 1.24. Внешний вид специального приемного устройства КПЛ

емник информации с диапазоном перестройки 1,6...2,2 МГц с фазовой модуляцией принимаемого сигнала. Габариты 110×56×21 мм, промежуточная частота 10,7 МГц, ширина полосы тракта SH4 180 кГц (рис. 1.24).

Другая группа радиозакладочных устройств с питанием от электросети предназначена для передачи информации по радиоканалу.

Удлинитель — радиозакладочное устройство, закамуфлированное под обычный удлинитель. Предназначено для контроля акустики помещения с передачей информации по радиоканалу. Напряжение питания 220 В, частота 50...60 Гц, время непрерывной работы не ограничено, рабочие частоты передачи: 108...130 МГц; 416...424 МГц, 470±10 МГц, WFM-, NFM-модуляция, дальность передачи 100...300 м, кварцевая стабилизация передатчика.

Фильтр сетевой предназначен для контроля акустики помещения с передачей информации по радиоканалу. Питание от электросети напряжением 220 В и частотой 50...60 Гц. Радиомикрофон закамуфлирован в обычный сетевого фильтра Pilot. Время непрерывной работы не ограничено, рабочие частоты передачи: 108...130 МГц; 416...424 МГц, 470+ 10 МГц, WFM-, NFM-модуляция, дальность передачи 100...300 м, кварцевая стабилизация передатчика.

Основы подготовки и выполнения поисковых работ будут рассмотрены в третьей главе, а сейчас рассмотрим основные демаскирующие признаки закладочных устройств. Любой вид электронных устройств негласного съема информации обладает своими демаскирующие признаки, позволяющие их обнаружить.

Демаскирующие признаки закладных устройств условно можно разделить на признаки внешнего вида, определяющиеся визуально, и признаки, определяющиеся с помощью специальной аппаратуры. Демаскирующие признаки внешнего вида:

- малогабаритный предмет (часто в форме параллелепипеда) неизвестного назначения;
- одно или несколько отверстий малого диаметра в корпусе;
- наличие автономных источников питания (например, аккумуляторных батарей);
- наличие небольшого отрезка провода (антенны), выходящего из корпуса;
- тонкий провод неизвестного назначения, подключенный к малогабаритному микрофону и выходящий в другое помещение.

Закамуфлированные закладочные устройства имеют вид предметов повседневного обихода с сохранением их функционального назначения. Камуфляж может быть разнообразен: наручные часы, зажигалка, авторучка, электронная фоторамка, пепельница и т. д.. Визуально они ничем не отличаются от обычных предметов бытового назначения. Нередко злоумышленники заменяют бытовые приборы и предметы интерьера, находящиеся в помещении, аналогичными, но оборудованные закладочными устройствами.

Подобные закладочные устройства не всегда представляется целесообразным или возможным выявить при разборке предмета, так как чаще всего места соединения разбираемых частей склеивают или заливают специальными составами. Такие закладочные устройства определяются при анализе специфических признаков с использованием специальной аппаратуры. Такими признаками может быть:

- наличие в линии (проводе) неизвестного назначения постоянного (в несколько вольт) напряжения и низкочастотного информационного сигнала;
- наличие полупроводниковых элементов;
- радиоизлучения с модуляцией радиосигнала информационным сигналом;
- наличие в линии электропитания высокочастотного сигнала (как правило, несущая частота от 40 до 600 кГц, но возможно наличие сигнала на частотах до 7 МГц), модулированного информационным низкочастотным сигналом;
- наличие тока утечки (от единиц до нескольких десятков мА) в линии электропитания при всех отключенных потребителях;
- отличие емкости линии электропитания от типовых значений при отключении линии от источника питания (на распределительном щитке электропитания) и отключении всех потребителей;
- радиоизлучения с модуляцией радиосигнала информационным сигналом, передаваемым по телефонной линии;
- отличие сопротивления телефонной линии от «бесконечности» при отключении телефонного аппарата и отключении линии (отсоединении телефонных проводов) в распределительной коробке (щитке);
- отличие сопротивления телефонной линии от типового значения (для данной линии) при отключении телефонного аппарата, отключении и закорачивании линии в распределительной коробке (щитке);
- падение напряжения (от нескольких десятых до 1,5...2 В) в телефонной линии (по отношению к другим телефонным линиям, подключенным к данной распределительной коробке) при положенной и поднятой телефонной трубке;

- наличие тока утечки (от единиц до нескольких десятков мА) в телефонной линии при отключенном телефоне.

1.4.6. Волоконно-оптические линии связи

Последние годы все больший интерес проявляется к использованию для передачи информационных сигналов волоконно-оптических линий связи (ВОЛС). Это вызывает необходимость более детально разобраться с особенностями функционирования волоконно-оптических линий связи.

Производители оптоволокна говорят о том, что несанкционированный съем информации при её передаче по ВОЛС практически невозможен. Поэтому необходимо разобраться, так ли это на самом деле.

Прежде всего рассмотрим, что же представляют собой ВОЛС и могут ли быть реализованы на них какие-либо угрозы по несанкционированному съему информации.

В основе оптоволоконных технологий лежит принцип использования света как основного источника информации. Свет намного проще, чем электрический ток, передать на дальние расстояния с меньшими потерями. Кроме того, он значительно меньше подвержен воздействию электромагнитных полей и способен передавать на порядки большее количество информации. Оптические линии сами не являются источниками электрических шумов. Высокая пропускная способность и быстродействие передачи электромагнитного излучения оптического диапазона обеспечивается за счет использования частотного диапазона $1014 \ldots 1015$ Гц.

Фактическое отсутствие в природе и промышленности источников электрического и магнитного поля напряженности, которые способны изменить условия распространения светового импульса в оптоволокне, обеспечивают высокую помехозащищенность ВОЛС. Кроме того, оптические кабели чаще всего не содержат металлических элементов, поэтому проблем, связанных с разностью потенциалов этажей и зданий, с блуждающими токами в почве и т. п., не возникает. Волоконно-оптические системы имеют почти полную электрическую изоляцию, не боятся повышенной влажности, не требуют оборудования, защищающего их от утечек, пробоев и короткого замыкания. Полупроводниковые приемники и передатчики света обладают достаточно высокой стабильностью.

Принципиальная схема передачи информации по ВОЛС представлена на рис. 1.25. При передаче информация, преобразованная в световую волну, подается в ВОЛС, а адресат, получая последнюю, в свою очередь, интерпретирует свет как информацию. Электрический

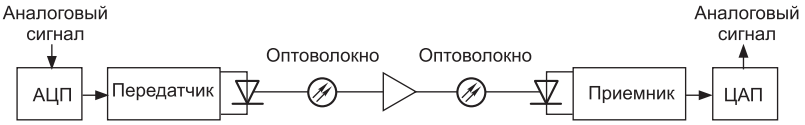


Рис. 1.25. Принципиальная схема передачи информации по ВОЛС

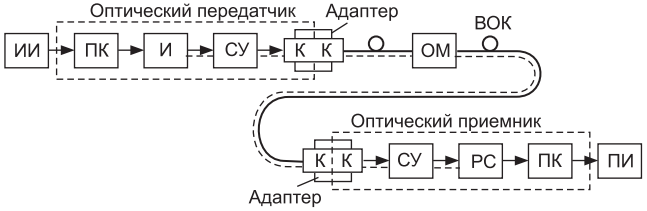


Рис. 1.26. Структурная схема волоконно-оптической линии связи: ИИ — источник информации; ПК — преобразователь кода; И — излучатель света; СУ — согласующее устройство (оптическое); К — коннектор оптический; ВОК — волоконно-оптический кабель; ОМ — оптическая муфта кабеля; ФД — фотодиод; РС — регенератор сигала; ПИ — приемник информации

сигнал поступает на вход оптического передатчика и модулирует интенсивность выходного сигнала излучателя. Оптический сигнал распространяется по волоконному световоду и поступает на вход оптического приемника, который осуществляет его демодуляцию и восстанавливает исходный электрический сигнал. Нормальная эксплуатация линий связи обеспечивается комплектацией оптических передатчиков и приемников розетками оптических разъемов. Структурная схема волоконо-оптической линии связи представлена на рис. 1.26.

Для анализа и оценки возможностей по съёму информации с ВОСП более подробно рассмотрим устройство и структуру оптических кабелей. По типу оптических волокон кабели подразделяются на одномодовые и многомодовые. Число оптических волокон в кабелях обычно от 4 до 216. Срок службы волоконно-оптических кабелей, как правило, не менее 25 лет. Устройства одномодового и многомодового оптических кабелей представлены на рис. 1.27.

Одномодовый кабель состоит из:

- сердечника *1* (core) (обычно из стекла, реже пластик), который используется для передачи светового сигнала, размером 9 или 50/62,5 мкм;
- отражающей оболочки *2* (cladding) с внешним диаметром 125±2 мкм, покрытой защитным лаком *5*;
- защитного покрытия *3* (buffer coating);
- вторичного буфера *4*.

Многомодовые кабели в своей структуре имеют:

1 — оптическое волокно;

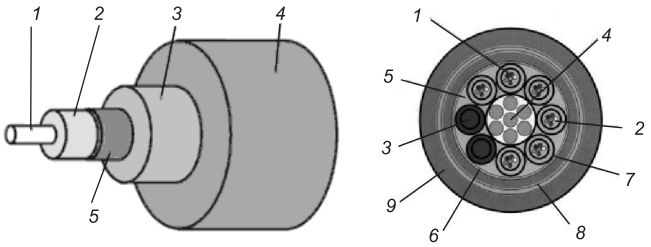


Рис. 1.27. Устройство одномодового и многомодового оптических кабелей

2 — внутримодульный гидрофобный заполнитель;
3 — кордель;
4 — центральный силовой элемент — стальной трос;
5 — гидрофобный заполнитель;
6 — скрепляющая лента;
7 — промежуточная оболочка из полиэтилена;
8 — броня из стальной гофрированной ленты;
9 — защитная оболочка из полиэтилена.

Современные оптоволоконные кабели в зависимости от предназначения имеют свои конструктивные особенности, что имеет существенное значение при анализе возможностей по несанкционированному съёму информации. Волоконно-оптические кабели в броне из круглых стальных оцинкованных проволок и защитном шланге из полиэтилена служат для прокладки через водные преграды, непосредственно в грунте, в кабельной канализации и других линейных сооружениях; небронированные волоконно-оптические кабели в полиэтиленовой оболочке — для прокладки в пластмассовых трубах и внутри зданий; волоконно-оптические кабели подвесные с выносным силовым элементом — для подвески на столбах освещения.

Такое разнообразие кабелей требует особого подхода к анализу возможностей по несанкционированному съёму информации с ВОЛС. На первый взгляд все очевидно. Оптоволокно — это обычное стекло, передающее электромагнитную энергию в виде света инфракрасного диапазона. Излучение наружу практически отсутствует. Перехватить сообщение можно, только физически подключившись к волокну. Таким образом, кажется, что проблема информационной безопасности окончательно решена. Когда поставщиков сетевых систем спрашивают о возможных решениях, они, как правило, отвечают: «Если вам требуется безопасность, используйте оптоволокно».

Однако не так все просто. Оптоэлектроника (особенно для поддержки высокоскоростных приложений, систем видеонаблюдения и видеоприложений) стоит дорого и во многих случаях не снимает проблемы излучения электромагнитной энергии в окружающее пространс-

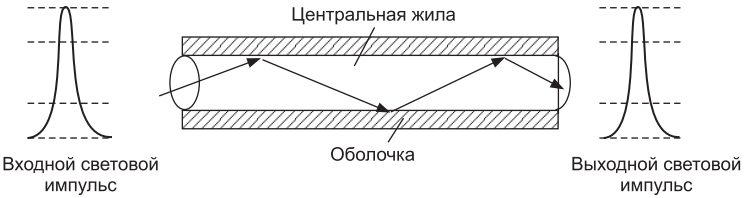


Рис. 1.28. Принципиальная схема распространения световой волны в одномодовом кабеле

тво, поскольку рабочие станции, серверы, интерфейсные карты, концентраторы и другие сетевые устройства также являются активным оборудованием и задают собственный уровень излучений. Поэтому, принимая решения об использовании оптоволоконных кабельных систем (ОКС), важно представлять фактическое состояние дел по вопросам безопасности.

Более детально рассмотрим принципы передачи информации по ВОЛС. В зависимости от решаемых задач используются одномодовые или многомодовые кабели. По одномодовым волокнам передаются оптические сигналы с одной длиной волны (рис. 1.28). Поэтому одномодовое волокно проектируется так, что в нем может распространяться только одна мода (диаметр сердечника обычно 9 мкм). Одномодовый кабель применяется для передачи сигналов на большие расстояния. Используемая длина волны 1310 или 1550 нм. Потери на волне 1310 нм около 0,4 дБ/км; на волне 1550 нм около 0,2 дБ/км.

У многомодового волокна диаметр сердечника (обычно 50 или 62,5 мкм) почти на два порядка больше, чем длина световой волны. Это означает, что свет может распространяться в волокне по нескольким независимым путям (модам). И так как разные моды имеют разную длину, то сигнал на приемнике будет заметно «размазан» по времени (рис. 1.29). Используемая длина волны 850 или 1310 нм. Потери на волне 850 нм около 3 дБ/км; на волне 1310 нм около 1 дБ/км.

В многомодовых волокнах могут передаваться сигналы с различной длиной волны. Для совмещения нескольких оптических сигналов применяется так называемый волновой мультиплексор (Wave Division

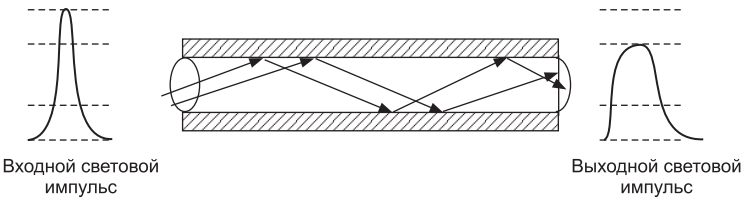


Рис. 1.29. Структура светового импульса в многомодовом кабеле

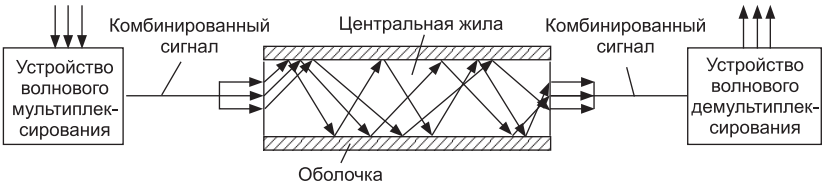


Рис. 1.30. Принцип мультиплексирования

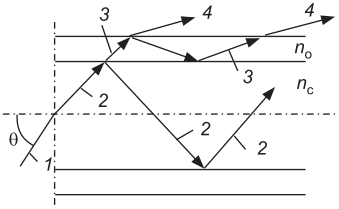


Рис. 1.31. Структура поля информационного оптического сигнала: θ — угол ввода оптического сигнала в волокно; n_c — показатель преломления сердцевины оптического волокна; n_o — показатель преломления оболочки оптоволокна; *1* — траектория луча (моды), вводимого в волокно; *2* — траектория луча (моды) передаваемого оптического информационного сигнала по сердцевине волокна; *3* — траектория луча (моды), передаваемого по оболочке волокна; *4* — траектория вытекающего луча (моды)

Multiplexer — WDM). WDM работает как призма. Сигналы с различной длиной волны комбинируются в нем, а затем пересылаются по одному из оптических волокон. Призма на приемном конце разлагает сигнал на волны исходной длины и направляет их на вход соответствующего оптического приемника.

Применение мультиплексирования позволяет увеличить число возможных каналов передачи данных (рис. 1.30).

Для оценки возможности по утечке информации рассмотрим структуру поля передаваемого информационного оптического сигнала (рис. 1.31).

Необходимо также отметить, что вытекающие моды в свою очередь делятся на слабозатухающие и быстрозатухающие моды.

В отличие от быстрозатухающих мод излучения, которые практически полностью затухают на трехметровом отрезке оптического волокна, слабозатухающие моды затухают сравнительно медленно и оказывают заметное влияние на измерения побочного излучения при длинах измеряемого отрезка кабелей до сотен метров. Например, в градиентных многомодовых волокнах с параболическим профилем около 25 % распространяемой энергии может содержаться в слабозатухающих модах.

С точки зрения утечки информации наиболее опасными являются оболочечные и вытекающие моды. Для съёма информации достаточно иметь доступ к данному типу оптического волокна и с помощью высокочувствительных фотоприемных устройств (в качестве оптического объектива можно использовать микролинзы или специ-

альное оптическое волокно, оптически согласованное с основным с помощью специально подобранной иммерсионной жидкости) можно принять передаваемый оптический сигнал.

В качестве излучателя для ВОСП могут использоваться полупроводниковые устройства двух типов. Устройство простейшего типа — светоизлучающий диод — имеет широкую диаграмму направленности излучения и поэтому пригодно для работы с многомодовыми волоконными световодами с большим диаметром сердцевины.

Более сложные устройства — полупроводниковые лазеры — излучают значительно лучше сколимированные пучки света и поэтому позволяют вводить сигнал более высокой мощности (в 10...100 раз) в многомодовые световоды, а также эффективно вводить сигнал в одномодовые световоды с малым диаметром сердцевины.

Светоизлучающие диоды вполне подходят для применения в информационных каналах и в системах связи с невысокой или умеренной пропускной способностью.

Таким образом, утечка информации у излучателя возможна:

- за счет несогласования геометрических размеров окна (микролинзы) светоизлучающего диода или полупроводникового лазера и торца (апертуры) волоконного световода;
- за счет окон прозрачности вокруг контактов на подложке, к которым подводится передаваемый информационный сигнал в радиочастотном диапазоне.

Числовая апертура волоконного световода определяется выражением

$$NA = \sqrt{n_{\text{с}}^2 - n_{\text{о}}^2},$$

где $n_{\text{с}}$ — показатель преломления сердцевины волоконного световода; $n_{\text{о}}$ — показатель преломления оболочки.

В качестве приемника в ВОСП, как правило, используются фотодиоды.

Следовательно, утечка у приемника в оптическом диапазоне частот возможна:

- за счет несогласования геометрических размеров окна (микролинзы) фотодиода и торца волоконного световода;
- за счет окон прозрачности вокруг контактов на подложке, к которым подводится принимаемый информационный сигнал в радиочастотном диапазоне.

Для исключения утечки информации в оптическом диапазоне частот у излучателя и приемника необходимо, чтобы их конструкция с физической точки зрения представляла абсолютно «черное тело», что довольно сложно реализовать на практике. Как правило, потери в оптических разъемах составляют 2,5...4,5 дБ.

Для передачи по одному оптоволокну одновременно нескольких независимых сигналов применяются методы временно́го и частотного уплотнения сигналов. Для этого в оптоволоконные системы наиболее часто устанавливают оптические мультиплексоры с частотным (спектральным) разделением каналов, которые объединяют несколько передаваемых сигналов в один.

Каждый источник сигнала передается лучами с различными длинами волн. Эти лучи проходят по оптоволоконной линии независимо и не взаимодействуют друг с другом. Такой вид модуляции называется WDM (wavelength division multiplexing). Он повышает пропускную способность оптоволоконной системы и позволяет осуществлять одновременную двунаправленную передачу информации, однако это не исключает возможности утечки информации.

Основные физические принципы формирования каналов утечки в ВОЛС можно разделить на следующие типы:

- нарушение полного внутреннего отражения;
- регистрация рассеянного излучения на длинах волн основного информационного потока и комбинационных частотах;
- параметрические методы регистрации проходящего излучения.

Анализируя основные физические принципы формирования каналов утечки, можно определить, как могут образовываться каналы утечки информации. Формирование каналов утечки возможно:

- при изменениях формы оптоволокна;
- при контактном и бесконтактном подключении к линиям волоконно-оптической связи;
- акустическим воздействием на оптическое волокно;
- за счет механического воздействия без изменения формы волокна;
- при бесконтактном подключении к ВОЛС;
- используя метод оптического туннелирования.

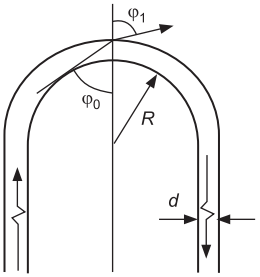


Рис. 1.32. Изменение формы оптоволокна

Изменение формы оптоволокна. Изменение угла падения может достигаться механическим воздействием на оптоволокно, например его изгибом (рис. 1.32). При изгибе оптического волокна происходит изменение угла падения электромагнитной волны на границе сердцевина-оболочка. Угол падения становится меньше предельно допустимого угла, что означает выход части электромагнитного излучения из световода. Изгиб оптического волокна приводит к сильному побочному излучению в месте изгиба, что создаёт возможность несанкционированного съёма информации в локализованной области.

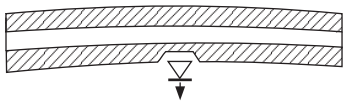


Рис. 1.33. Контактное подключение

Контактное подключение к линиям волоконно-оптической связи. Для контактного подключения удаляют защитный слой кабеля, стравливают светоотражающую оболочку и изгибают оптический кабель на необходимый угол (рис. 1.33). При таком подключении к ВОЛС обнаружить утечку информации за счет ослабления мощности излучения бывает очень трудно, так как, чтобы прослушать переговоры при существующих приемных устройствах несанкционированного доступа, достаточно отобрать всего 0,001 % передаваемой мощности. При этом дополнительные потери, в зависимости от изгиба кабеля, составляют всего 0,01...1,0 дБ.

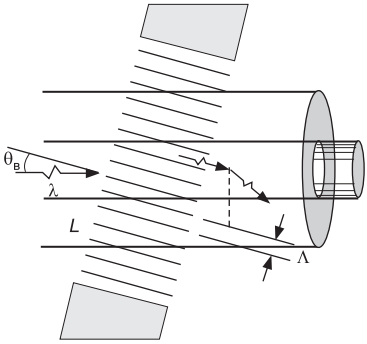


Рис. 1.34. Акустическое воздействие на оптическое волокно

Акустическое воздействие на оптическое волокно. Изменения угла падения можно добиться и акустическим воздействием на оптическое волокно (рис. 1.34). В сердцевине оптоволокна создаётся дифракционная решётка периодического изменения показателя преломления, которая вызвана воздействием звуковой волны. Электромагнитная волна отклоняется от своего первоначального направления, и часть её выходит за пределы канала распространения. Деформации, создаваемые упругой волной, формируют периодическое изменение показателя преломления внутри оптоволокна, являющегося дифракционной решёткой.

Механическое воздействие без изменения формы волокна. Другим внешним воздействием, изменяющим отношение показателя преломления оболочки к показателю преломления сердцевины оптоволокна (n_2/n_1), является механическое воздействие без изменения формы волокна, например растяжение (рис. 1.35).

К способам, вызывающим изменение отношения показателя преломления оболочки к показателю преломления сердцевины оптоволокна механическим напряжением, также относится скручивание оптоволокна.

Бесконтактное подключение к ВОЛС (рис. 1.36) осуществляется следующим образом:

- в качестве элемента съема светового сигнала используется стеклянная трубка, заполненная жидкостью с высоким показателем преломления и с изогнутым концом, жестко фиксированная на

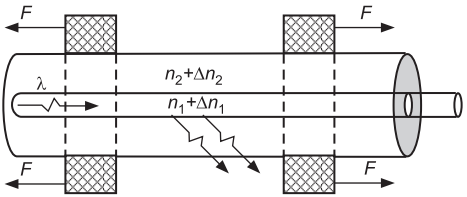


Рис. 1.35. Механическое воздействие растяжением

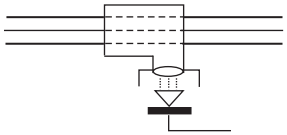


Рис. 1.36. Бесконтактное подключение к ВОЛС

оптическом кабеле, с которого предварительно снята экранная оболочка;

- на отогнутом конце трубки устанавливается объектив, фокусирующий световой поток на фотодиод, а затем этот сигнал подается на усилитель звуковых сигналов.

Метод оптического туннелирования. Способ, позволяющий захватывать часть электромагнитного излучения, выходящего за пределы сердцевины информационного оптического волокна, дополнительным световодом, не внося дополнительных потерь и обратного рассеяния, называется оптическим туннелированием (рис. 1.37).

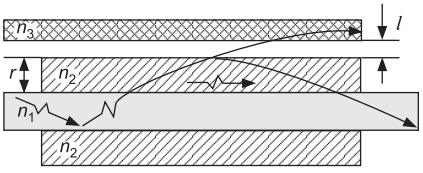


Рис. 1.37. Схема оптического туннелирования

Явление оптического туннелирования состоит в прохождении оптического излучения из среды с показателем преломления n_1 через слой с показателем преломления n_2 меньшим n_1 в среду с показателем преломления n_3 при углах падения больших угла полного внутреннего отражения. На принципах оптического туннелирования в интегральной и волоконной оптике создаются такие устройства, как оптический ответвитель, оптофоны, волоконно-оптические датчики физических величин.

Широкое распространение волоконно-оптических систем связи создаёт новые угрозы в защите информации, внимание к которым не является достаточным. При разработке и монтаже новых структурированных кабельных систем с волоконно-оптическими элементами основное внимание обращается на защиту трафика информационной системы от несанкционированного съёма, при этом угрозы другим видам информации остаются за рамками мероприятий по информационной безопасности.

Одной из таких угроз является возможность несанкционированного съёма конфиденциальной речевой информации с использованием локальных волоконно-оптических кабельных систем, проложенных

внутри помещений, зданий, территорий. Волоконно-оптический кабель локальных информационных систем может проходить через технические и специальные помещения коммерческих и государственных учреждений, защищаемые от утечки речевой информации. В существующих инструкциях, рекомендациях и аналитических обзорах по информационной безопасности формирование канала утечки конфиденциальной речевой информации не обсуждается.

В случае использования оптоволокна для несанкционированного съёма конфиденциальной речевой информации технические средства разведки включают описание физических принципов звуковой модуляции оптического потока в световоде и последующей демодуляции. Распространяющийся в воздушной среде информативный звуковой сигнал воздействует на оптическое волокно с передаваемым оптическим сигналом данных. Акустическая волна, как и волна механическая, воздействует на все элементы технических конструкций, расположенных на её пути, в том числе и на элементы волоконно-оптических коммуникаций, что приводит к модуляции интенсивности оптического излучения в канале связи звуковым сигналом. Промодулированное звуком световое излучение в оптоволокне выходит за пределы охраняемой зоны и может быть принято нарушителем. Описанный способ съёма информации можно назвать акусто-оптоволоконным каналом утечки.

Принципы реализации акусто-оптоволоконного канала утечки. Обеспечить функционирование акусто-оптоволоконного канала утечки можно при условиях, когда световой поток или уже существует, или специально создаётся в кабельной сети. Реализация каждого из способов зависит от режима работы активного оборудования и может быть разделена на два вида по состоянию сетевого оборудования:

- режим активного состояния сетевого оборудования;
- режим пассивного состояния сетевого оборудования.

Каждый из режимов имеет свои особенности и требует отдельного обсуждения, но физические принципы остаются неизменными, причём переход с одного режима на другой не предусматривает необходимости конструктивных изменений канала утечки в месте акустической модуляции. Особенностью активного состояния является возможность формирования канала утечки без выключения сетевого оборудования, используя внешний источник света, который смещён по частоте от применяемой в линии связи. Вывод дополнительной конфиденциальной речевой информации может быть осуществлен специальными методами или изменением параметров работы коммуникационного оборудования. В первом случае требуется установка в незащищённых помещениях рядом с источником речевой информации специального считывающего акустическую информацию устройс-

Рис. 1.38. Программно-аппаратный комплекс «Лазурит»

тва, а также создание отдельного канала передачи данных за пределы комнаты или её накопление на месте считывания. Во втором — необходимо провести перепрограммирование активного сетевого оборудования, а для передачи данных может быть использована та же самая локальная информационная сеть с выходом на незащищённый участок, где информация накапливается и забирается нарушителем.

Такое количество потенциальных каналов утечки информации при её передаче по ВОЛС вызывает необходимость разработки и применения технических средств для выявления каналов утечки и защиты информации от утечки по выявленным каналам.

Так как по сути вопросы защиты оптоволокна в литературе такого типа практически не рассматривались, то есть необходимость более детально рассмотреть их. В настоящее время вопросам защиты ВОЛС стали уделять внимание производители средств обнаружения возможных каналов утечки и средств защиты информации. На рынке появилось оборудование способное выявлять каналы утечки и закрывать их.

«Лазурит» — программно-аппаратный комплекс для измерения параметров волоконно-оптических систем передачи и оценки защищенности оптических линий связи (рис. 1.38) — предназначен для измерения параметров волоконно-оптических систем передачи и оценки защищенности оптических линий связи.

В комплексе заложены возможности оптического тестера и рефлектометра. Аппаратура комплекса позволяет выполнять измерение мощности оптического излучения, измерение затухания в оптических волокнах и их соединениях, определение длин волоконно-оптических линий, локализацию неоднородностей и соединений волокна, включая те, которые вызваны поломкой кабеля, визуально определять места повреждения волокна, генерировать стабилизированное оптическое излучение. Кроме того, комплекс позволяет осуществить автоматический расчет параметров защищенности и формировать финальный протокол измерений и расчетов. Комплекс может работать

в автоматизированном и ручном режимах. Наличие одномодового и многомодового рефлектометра в одном приборе позволяет осуществлять проверку и анализ одномодовых и многомодовых ВОЛС. Наличие удаленного управления, автономного и внешнего источника питания позволяет проводить работы с комплексом как в лабораторных, так и полевых условиях. Комплекс имет источник внешнего излучения.

Набор пассивных устройств (ответвителей, аттенюаторов), соединительных кабелей и адаптеров обеспечивает проведение измерений по схемам, предложенным в нормативно-методических документах.

Комплекс технических средств контроля несанкционированного доступа к оптическим волокнам (КТС ОВ, рис. 1.39) предназначен для обнаружения попыток несанкционированного подключения к контролируемым оптическим волокнам.

Диагностика оптических волокон осуществляется сравнением текущего и исходного значения потерь в оптическом волокне и сопоставлением найденных отклонений с заданным пороговым значением. Контроль осуществляется в рабочих волокнах, передача информации и измерения производятся на разных длинах волн.

Рис. 1.39. Комплекс технических средств контроля НСД к оптическим волокнам

При изменениях потерь в информационном канале появляются предупредительные сигналы:

- «Тревога» — при приближении уровня потерь к пороговому значению;
- «Блокировка» — при превышении значений уровня установленного порога, при этом КТС ОВ обеспечивает переключение информационного сигнала на резервный канал.

КТС ОВ обеспечивает возможность установки уровня мощности передаваемого оптического информационного сигнала ниже уровня, при котором возможен перехват информации.

КТС ОВ состоит из двух идентичных оптоэлектронных приёмопередающих устройств.

Оптоэлектронные приёмо-передающие устройства включаются в разрыв оптических линий связи таким образом, чтобы информационный и контрольный оптические сигналы распространялись по ОВ навстречу друг другу.

Программно-аппаратный комплекс «Шлюз» (рис. 1.40) предназначен для организации однонаправленной передачи информации из сегмента ЛВС, подключённого к Интернету (открытый сегмент), в

Рис. 1.40. Программно-аппаратный комплекс «Шлюз»

сегмент ЛВС, в котором происходит обработка и хранение информации ограниченного пользования (закрытый сегмент).

ПАК «Шлюз» изготовлен в соответствии с «Требованиями по защите конфиденциальной информации от несанкционированного доступа в автоматизированных системах, расположенных на территории Российской Федерации» по классу АК3. В составе ПО ПАК «Шлюз» используется средство антивирусной проверки файлов, поступающих из открытого сегмента, соответствующее классу В2 «Требований к антивирусным средствам ФСБ РФ». Для защиты от сетевых атак в ПАК «Шлюз» используется межсетевой экран, удовлетворяющий 4 классу «Временных требований к устройствам типа межсетевые экраны». Контроль целостности программного обеспечения ПАК «Шлюз» обеспечивается аппаратно-программным модулем доверенной загрузки (АПМДЗ), сертифицированного ФСБ России.

Рис. 1.41. Устройство защиты «Фотон-М»

Устройство защиты «Фотон-М» (рис. 1.41) предназначено для защиты акустической информации, циркулирующей в выделенных (категорированных) помещениях, от утечки за счет акустооптических преобразований, возникающих в волоконно-оптической линии связи, проложенной в помещении, и в элементах оптического сетевого интерфейса ПЭВМ, подключенной к ВОЛС, а также от утечки акустической информации за счет преднамеренно внедренных в оптоволоконную линию связи оптических микрофонов.

«Фотон-М» устанавливается в границах контролируемой зоны вне категорированного помещения на выходе оптоволоконной линии из категорированного помещения в некатегорированное или в помещение с более низкой категорией, в условиях отсутствия воздействия защищаемой речевой информации на участок оптоволоконной линии, расположенный после устройства защиты «Фотон-М».

Устройство обеспечивает защиту от:

- акустооптических преобразований на рабочей длине волны оптического сигнала, излучаемого ТСОИ, установленного в помеще-

нии, а также на длине волны преднамеренно внедренного оптического микрофона;

- акустооптических преобразований на длине волны зондирующего оптического сигнала, отличающейся от рабочей длины волны ТСОИ и подающегося в оптоволокно из точки, находящейся вне контролируемой зоны;
- акустооптических преобразований в оптоволокне, проходящем транзитом через защищаемое помещение.

Если оптоволоконная линия входит из незащищаемого помещения и выходит в незащищаемое помещение, то устройство защиты должно устанавливаться с двух сторон.

Устройство может применяться в ВОСП, используемых для передачи данных оборудованием сетей Ethernet, соответствующим стандартам 802.3j, 802.3u, 802.3z, а также обобщенному стандарту IEEE 802.3-2005. Выпускаются устройства различной модификации исходя из типа оптоволоконной линии — одномодовая или многомодовая, длины волны оптического сигнала — 850 нм, 1310 нм, 1550 нм, скорости передачи данных — 10, 100 и 1000 мегабит в секунду, а также способа передачи данных — по одному оптоволокну в одну сторону, по второму в другую на одной и той же длине волны или по одному оптоволокну в обе стороны на разных длинах волн оптического сигнала. Возможна комбинация в одном устройстве различных типов оптоволокна, длин волн и скоростей передачи данных.

Конструктивно устройство выполнено в виде блока, устанавливаемого в 19-дюймовую стойку, и может занимать от 1 до 3 юнитов.

Блок размером в 1 юнит имеет от 1 до 6 каналов, размером в 2 юнита — от 7 до 12 каналов, размером в 3 юнита — от 13 до 18 каналов.

Также изделие может быть выполнено в виде отдельного устройства с элементами крепления к стене или установки на столе.

Аттенюатор оптический перестраиваемый (рис. 1.42) предназначен для внесения оптического затухания в волоконно-оптические системы передачи информации, реализованные на одномодовом волокне на длине волны 1,55 мкм, а также для оценки качества волоконно-оптических систем связи.

Рис. 1.42. Аттенюатор оптический перестраиваемый

В аттенюаторе предусмотрена возможность регулировки с высокой точностью вносимого затухания до 0,01 дБм. Простая регулировка, малые габариты и вес. Рабочая длина волны 1,55±0,05 мкм. Диапазон регулировки оптического затухания на длине волны 1,55±0,05 мкм от

2 до 30 дБ. Диапазон рабочих температур от −30 до + 50 °С. Нестабильность оптического затухания в диапазоне рабочих температур не более 2 %. Тип присоединяемых оптических разъемов — FC. Количество присоединяемых оптических разъемов 2. Возвратные потери при использовании оптических разъемов FC/APC не менее 60 дБ.

В рамках данного пособия не стояла задача подготовить специалистов по защите от утечки информации через ВОЛС. В пособии сделана попытка обратить внимание специалистов на появление сравнительно новых технических каналов утечки информации, при использовании перспективных ВОЛС и необходимость защиты информации от утечки по данным каналам.

1.4.7. «Легальные» закладочные устройства

Рассматривая вопросы несанкционированного съема информации с помощью закладочных устройств, нельзя не остановиться на стремительно развивающемся направлении незаконного получения информации с использованием так называемых «легальных» закладочных устройств — диктофонов и сотовых телефонов.

При использовании систем сотовой связи для получения информации необходимо обратить внимание на появление на рынке закладочных устройств, разработанных на базе SIM-карт сотовых телефонов, которые позиционируются продавцами как охранное средство контроля акустики помещения. Такие устройства имеют до четырех чувствительных микрофонов, которые позволяют получить речевую информацию из помещения, где находится данное устройство. Закладочное устройство переходит в режим ожидания после установки в него SIM-карты. При наборе номера по сотовому телефону устройство активируется и позволяет принимать акустическую информацию, циркулирующую в защищаемом помещении. По своим геометрическим размерам данные устройства сравнимы с цифровыми закладочными устройствами (рис. 1.43).

Таким образом, в современных условиях дорогостоящие предварительные проверки помещений на наличие подслушивающей аппа-

Рис. 1.43. Общий вид ЗУ на базе SIM-карты сотового телефона

ратуры и технических каналов утечки информации, предшествующие обсуждению в этих помещениях конфиденциальных вопросов, теряют смысл в случае проноса аппаратуры несанкционированного получения информации непосредственно участником переговоров.

1.4.8. Диктофоны

Благодаря бурному развитию электроники малогабаритные диктофоны обладают хорошими эксплуатационными характеристиками, позволяющими записывать информацию с высоким качеством в самых сложных условиях акустической обстановки в автоматическом режиме. Многообразие типов диктофонов, от аналоговых устройств широкого применения до профессиональных цифровых, позволяет удовлетворить любые потребительские требования для проведения планируемых мероприятий. Сложность задачи обнаружения современных диктофонов заключается в том, что, с одной стороны, требуется регистрировать очень слабое электромагнитное излучение работающего диктофона, т. е. необходим достаточно чувствительный измеритель электромагнитных сигналов. С другой стороны, обнаружитель диктофонов не должен реагировать на помехи и на излучения других приборов, которые могут быть очень сильными. При этом частотный диапазон, характер и форма электромагнитных колебаний от диктофона и от мешающих источников одинаковы.

Единственным демаскирующим признаком для записывающего диктофона является его электромагнитное излучение. В зависимости от типа диктофона и характера его работы оно существенно отличается друг от друга. По создаваемому электромагнитному излучению диктофоны условно можно разделить на две группы: имеющие в своей конструкции электродвигатель и имеющие микросхемы памяти для записи информации.

К первой группе относятся следующие аппараты ,построенные на:

- классическом принципе записи электрических сигналов на магнитную ленту в аналоговом виде, имеющих лентопротяжный механизм и не имеющие генератора стирания и подмагничивания (ГСП);
- классическом принципе записи электрических сигналов на магнитную ленту в аналоговом виде и подразумевающие наличие лентопротяжного механизма и имеющие ГСП;
- принципе записи электрических сигналов на магнитную ленту в цифровом виде и имеющие лентопротяжный механизм, аналогичный механизму видеомагнитофона;
- принципе записи электрических сигналов на магнитный или оптический дисковый носитель в цифровом виде или на лазерный перезаписываемый диск (оптический носитель). Также имеют электродвигатель.

Теоретически цифровым диктофоном является устройство, осуществляющее запись речевой информации на некоторый носитель в цифровом виде. Однако, так как определяющим при поиске является характер электромагнитного излучения, а у всей этой группы оно имеет одинаковый характер из-за наличия электродвигателя, то условно назовем их кинематическими диктофонами.

Источниками максимального излучения этой группы являются электродвигатель и ГСП (только для второй подгруппы). Электродвигатель излучает сигнал импульсного характера с основной гармоникой в диапазоне от 80 до 300 Гц. В этом же диапазоне находятся и другие гармонические составляющие этого сигнала, но они имеют меньшие амплитуды. Излучение от ГСП приближено к синусоидальному и находится в пределах от 20 до 60 КГц.

Другая группа диктофонов построена на принципе записи электрических сигналов в кристалл микросхемы памяти в цифровом виде. При этом, как правило, используется энергонезависимая память (флэш-память), реже динамическая или статическая память, требующая постоянно подключенного источника питания. Эту группу диктофонов условно назовем цифровыми.

Конструктивно цифровые диктофоны могут быть выполнены в двух вариантах:

- функция диктофона является основной;
- функция диктофона является дополнительной.

Ко второй подгруппе относятся практически все сотовые телефоны, смартфоны типа iPhone и карманные миникомпьютеры, например PocketPC, а также современные MP3-плейеры с возможностью записи.

По характеру излучения цифровые диктофоны можно разделить на подгруппы:

- имеющие импульсный преобразователь напряжения;
- имеющие съемную конструкцию флэш-памяти;
- диктофоны, у которых сжатие речевой информации осуществляет специализированный сигнальный процессор;
- имеющие жидкокристаллический дисплей;
- имеющие различные подключенные аксессуары, такие как выносной микрофон, пульт дистанционного управления и т. д.;
- имеющие корпус, способный экранировать излучение диктофона.

Проведенные исследования позволили сделать вывод, что максимальный уровень излучения цифровых диктофонов для всех подгрупп, как правило, лежит в диапазоне от 20 до 120 кГц. Для диктофонов с импульсным преобразователем напряжения наиболее сильный уровень наблюдается на частоте преобразования. Такие диктофоны могут обнаруживаться на максимальной дальности — более метра.

В диктофонах со съемной флэш-памятью неизбежно присутствует шлейф из нескольких десятков проводников длиной несколько сантиметров. По нему передаются сигналы адреса и данных для записи в память. Эти сигналы цифровые, следовательно, имеют крутые фронты и амплитуду, равную напряжению питания (обычно 3 вольта). Наличие длинных проводников с такими сигналами дает шумоподобные всплески в некоторых частотных областях. Когда используется сигнальный процессор, спектральные всплески усиливаются, так как такой процессор потребляет более 50 % энергии, необходимой для работы диктофона. Диктофоны этих двух подгрупп могут обнаруживаться на расстоянии от 50 см до 1 м.

Диктофон с жидкокристаллическим дисплеем также является источником образования электромагнитного поля. Причем его энергия растет с увеличением размеров дисплея, а также в случае, если он графический и особенно цветной. Наличие таких дисплеев характерно для приборов, у которых функция диктофона является дополнительной, — сотовые телефоны, смартфоны, планшеты и т. д. Дальность обнаружения таких устройств может превысить 1 м.

Для диктофонов с подключенным выносным микрофоном или пультом дистанционного управления соединительный кабель является дополнительным относительно мощным источником излучения.

Для диктофонов в металлических корпусах дальность обнаружения резко падает, так как излучение экранируется корпусом, и в зависимости от качества экранирования составляет от нескольких единиц до 30 см. Однако существует вероятность образования низкочастотных субгармоник, от излучения которых экранирование малоэффективно. В любом случае диктофоны в металлических корпусах, как правило, относятся к классу спецтехники и специально разрабатываются с целью минимизации излучения.

С точки зрения электротехники диктофон состоит из набора замкнутых электрических цепей, причем некоторые из них обладают значительной индуктивностью, что приводит к образованию вокруг работающего диктофона электромагнитного излучения с определенной диаграммой направленности и интенсивностью. Отсюда следует вывод, что любой диктофон может быть обнаружен некоторым специальным электронным устройством на определенном расстоянии.

1.4.9. Сотовые телефоны

С точки зрения так называемых тактических возможностей сотовый телефон, при наличии «злого умысла», также может приобрести свойства устройств негласного съема информации, что вызывает необходимость рассмотрения основных понятий и принципов функционирования этого вида связи. При изучении данного вопроса сначала

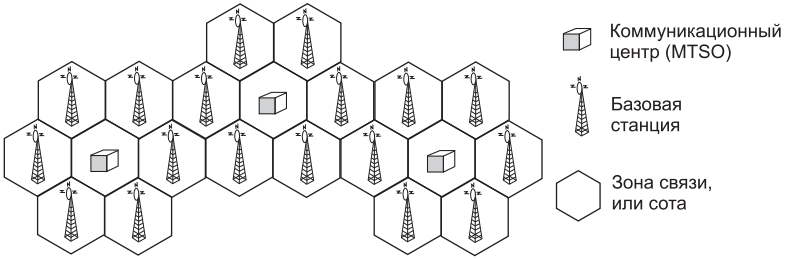


Рис. 1.44. Принципиальная схема сотовой связи

рассмотрим принципиальные основы осуществления связи без раскрытия технических деталей функционирования того или иного компонента, динамику развития этого вида связи, а затем изучим структуру и функционирование основных систем сотовой связи. Наша задача понять принципы построения системы подвижной связи и обратить внимание на те элементы, которые могут способствовать несанкционированному съему информации при работе сотовой связи.

Принципы работы сотовой связи. Система сотовой связи строится в виде набора ячеек, покрывающих обслуживаемую территорию (рис. 1.44). Ячейки системы принято схематически изображать в виде правильных шестиугольников подобно пчелиным сотам. Типичный радиус ячейки — от полукилометра до нескольких километров. В центре каждой ячейки находится базовая станция, которая обслуживает всех абонентов в пределах ячейки.

Все базовые станции замыкаются на центр коммутации, или коммутатор (многопроцессорная система, осуществляющая коммутацию потока информации и управления работой системы сотовой связи). С него также имеются выходы на другие системы и сети связи — городскую телефонную сеть, междугороднюю и международную сети связи, другие системы сотовой связи.

Связь между абонентами и базовыми станциями осуществляется по радиоканалам (через эфир), между базовыми станциями и центром коммутации, так же как и между центром коммутации и другими сетями связи, — по оптоволоконным, радиорелейным или проводным линиям связи.

Для того чтобы абонент мог получить адресованный ему вызов, центр коммутации должен располагать информацией о том, в какой ячейке он находится, чтобы понять через какую базовую станцию следует направить ему вызов. Вот почему телефоны абонентов периодически регистрируются в сотовой системе, посылая через ближайшую базовую станцию служебные сигналы на центр коммутации. При перемещении абонентов между ячейками последовательные регистрации происходят через разовые базовые станции, благодаря чему

центр коммутации располагает информацией о текущем местоположении абонентов.

Регистрация производится автоматически, но только при включенной «трубке» и в промежутках между сеансами связи. Если абонент пересекает границу смежных ячеек в ходе телефонного разговора, то происходит передача обслуживания от одной базовой станции к другой. Передача обслуживания происходит автоматически, без прерывания связи и практически незаметно для разговаривающих абонентов.

Коммуникационный центр — это мозг сети. Его главный компьютер управляет сотнями тысяч соединений в зоне, обслуживаемой данным центром. Центр MTSO назначает частоты для радиосвязи базовым станциям и подвижным радиотелефонам, а также распределяет вызовы в пределах своей зоны между сотовой сетью и обычными телефонными станциями общего пользования.

Базы данных сотовой сети содержат информацию как о местонахождении всех ее клиентов, так и об интерфейсах с другими такими же сетями, что необходимо для идентификации абонентов и проверки их права на доступ в сеть.

Базовая станция управляет телефонным обменом в своей зоне и способна принимать и передавать сигналы на большом количестве радиочастот. Она подключена к обычной проводной телефонной сети и оснащена аппаратурой преобразования высокочастотного сигнала сотового телефона в низкочастотный сигнал проводного телефона и наоборот, для обеспечения сопряжения обеих систем.

Периодически (с интервалом 30...60 минут) базовая станция излучает служебный сигнал. Мобильный телефон принимает сигнал, автоматически добавляет к нему свои мобильный идентификационный номер (MIN) и электронный серийный номер (ESN) и передает получившуюся кодовую комбинацию на базовую станцию. В результате этого осуществляется идентификация конкретного сотового телефона, номера счета его владельца и привязка аппарата к определенной зоне, в которой он находится в данный момент.

Когда пользователь звонит по своему телефону, базовая станция выделяет ему одну из свободных частот той зоны, в которой он находится, вносит соответствующие изменения в его счет и передает его вызов по назначению.

Радиопередатчики («мобильники», телефонные трубки). Мобильники — это миниатюрная приемопередающая радиостанция. Каждому сотовому телефонному аппарату присваивается ESN, который кодируется в микрочипе телефона при его изготовлении и сообщается изготовителями аппаратуры специалистам, осуществляющим его обслуживание. Кроме того, некоторые изготовители указывают этот

номер в руководстве для пользователя. При подключении аппарата к сотовой системе связи в микрочип телефона заносится еще и MIN.

Большинство систем сотовой связи работают по одному из стандартов: аналоговой (AMPS, TAGS, NTS и т. п.) или цифровой связи (D-AMPS, NMT, GSM и т. п.). Стандарты NMT-450 и GSM приняты в качестве федеральных, а AMPS/D-AMPS был ориентирован на региональное использование. Стандарт DCS-1800 является перспективным. В стандарте NMT-450 используется дуплексный разнос частот 10 МГц. Используя сетку частот через 25 кГц, система поддерживает 180 каналов связи. Радиус соты 15...40 км. Все служебные сигналы в системе NMT являются цифровыми и передаются со скоростью 1200/1800 бит/с FFSK (Fast Frequency Shift Keying). Сотовые системы, основанные на стандарте NMT, использовались в Москве, Санкт-Петербурге и в других регионах страны. Система сотовой связи стандарта AMPS работает в диапазоне 825...890 МГц и имеет 666 дуплексных каналов при ширине канала 30 кГц. В системе применяются антенны с шириной диаграммы направленности 120°, устанавливаемые в углах ячеек. Радиусы сот 2...13 км [48].

В России системы по стандарту AMPS были установлены более чем в 40 городах (Архангельск, Астрахань, Владивосток, Владимир, Воронеж, Мурманск, Н. Новгород и др.). В настоящее время AMPS практически заменен цифровыми стандартами. Цифровая система D-AMPS с использованием технологии множественного доступа TDMA в настоящее время самая распространенная из цифровых сотовых систем в мире. Цифровой стандарт имеет ширину частотного канала 30 кГц. Стандарт D-AMPS принят как региональный стандарт. По этому стандарту были созданы системы в Москве, Омске, Иркутске, Оренбурге. Стандарт GSM тесно связан со всеми современными стандартами цифровых сетей, в первую очередь с ISDN (Integrated Services Digital Network) и IN (Intelligent Network). В стандарте GSM используется узкополосный многостанционный доступ с временным разделением каналов (TDMA). В структуре TDMA кадра содержится 8 временных позиций на каждой из 124 несущих [48].

Для защиты от ошибок в радиоканалах при передаче информационных сообщений применяется блочное и сверточное кодирование с перемежением. Повышение эффективности кодирования и перемежения при малой скорости перемещения подвижных станций достигается медленным переключением рабочих частот (SFH) в процессе сеанса связи со скоростью 217 скачков в секунду.

Структуру сети сотовой подвижной связи более детально рассмотрим на примере стандарта GSM как наиболее распространенного стандарта для реализации речевых услуг.

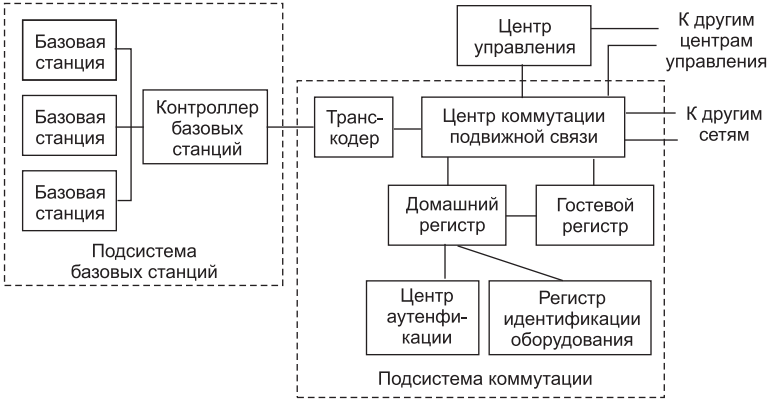


Рис. 1.45. Структурная схема базовой конфигурации и сети

Сети сотовой подвижной связи (СПС) представляют собой комбинированную структуру, состоящую из разного рода проводных сред (т. е. радио- и проводная связь). Такое объединение подразумевает сложную структуру сети, включающую приемное оборудование, транзитные узлы, конвекторы потоков, среду передачи данных. На рис. 1.45 приведена структурная схема базовой конфигурации сети СПС стандарта GSM [51].

Рассмотрим отдельные элементы сети GSM и их функциональное назначение.

Центр аутентификации (АиС) хранит данные о каждой абонентской станции, которые позволяют выполнить процедуру аутентификации и генерацию ключа шифрования сеанса связи. Назначение центра аутентификации оговорено в соответствующих рекомендациях, однако в большинстве случаев при проектировании и построении сетей СПС функции аутентификационного центра передаются домашнему регистру [51].

Домашний регистр (HLR), или регистр местоположения, предназначен для хранения данных о мобильных абонентах (абонентских станциях), постоянно зарегистрированных в данном центре коммутации. Функционально домашний регистр представляет собой базу данных, предназначенную для управления абонентскими станциями (АС). Количество домашних регистров в сети стандарта GSM зависит от числа АС, емкости используемого оборудования и организации сети.

В базе данных домашнего регистра хранится следующая информация:

- местоположение мобильной станции;
- международный идентификатор мобильной станции;
- тарифный план, используемый абонентом;

- виды подключенных услуг;
- ограничения на обслуживание абонента;
- идентификатор группового или широковещательного вызовов.

Гостевой регистр (VLR), или регистр местоположения, используется центром коммутации для получения информации, например, при управлении входящими (исходящими) вызовами временных (роумерных) АС.

Если абонентская станция находится на территории центра коммутации, где она еще незарегистрирована, то управление будет проводиться с помощью гостевого регистра. Когда АС переходит в новую зону обслуживания, запускается процедура регистрации. При этом центр коммутации, в зоне действия которого осуществляется регистрация, передает в гостевой регистр идентификатор области расположения роумерной АС. Дальнейшее управление абонентской станцией в зоне данного центра коммутации осуществляется посредством гостевого регистра. Структура гостевого регистра идентична структуре домашнего регистра, однако дополнительно вносятся следующие данные о АС:

- роуминговый номер АС;
- временный идентификатор АС;
- идентификатор местной АС;
- область расположения, в которой АС регистрировалась последний раз.

Основным отличием гостевого регистра от домашнего является то, что информация об абонентской станции хранится в нем, только если она находится в зоне его обслуживания. При выходе АС из зоны обслуживания вся информация о ней в гостевом регистре удаляется. В домашнем регистре информация о базовой станции (БС) хранится постоянно и передается гостевым регистрам других центров коммутации по запросу сети.

Регистр идентификации оборудования (EIR) предназначен для хранения международных идентификаторов мобильного оборудованияи идентификации оборудования по спискам «белого», «серого» или «черного» оборудования.

Стоит отметить, что данный функциональный элемент сети не реализован в полной мере в сетях отечественных операторов сотовой связи. Это связано с тем, что на этапе проектирования сетей использование регистра посчитали нецелесообразным и экономически невыгодным. Внедрить этот элемент сети можно и сейчас, но это повлечет за собой большие затраты на переоборудование сети и перераспределение данных внутри сети, с чем не все операторы могут согласиться. Регистр идентификации оборудования является эффективным средством борьбы с ворованными телефонами и может участвовать как

дополнительный элемент в механизме аутентификации абонента, поэтому уже сегодня наблюдается его внедрение в региональных сетях СПС в порядке эксперимента [51].

Центр коммутации подвижной связи (MSC) обеспечивает взаимодействие сети СПС с фиксированными сетями, а также выполняет все необходимые функции для управления вызовами мобильных станций.

Основной задачей центра коммутации мобильной связи является распределение радиоресурсов сети GSM, а также выполнение процедур, связанных с регистрацией местоположения и процедур, связанных с передачей эстафеты связи (handover). Кроме того, центр коммутации выполняет важную функцию межсетевого взаимодействия, которая обеспечивает взаимодействие сети GSM с фиксированными сетями. Эта функция зависит от типа фиксированной сети и запрашиваемого обслуживания.

Центр коммутации может также выполнять функции шлюза для другого центра коммутации сети, к которому приписан вызываемый абонент. Это происходит следующим образом: если сеть, передающая вызов в сеть GSM, не может запросить напрямую домашний регистр, вызов направляется напрямую к центру коммутации (шлюзу). Данный центр коммутации в свою очередь будет запрашивать соответствующий домашний регистр и затем направлять вызов к тому центру коммутации, в зоне действия которого последний раз регистрировался искомый абонент.

Контроллер базовой станции (BSC) — элемент сети GSM, предназначенный для управления одной или несколькими базовыми станциями.

Базовая станция (БС) — элемент сети GSM, обеспечивающий работу абонентских станций в зоне радиопокрытия одной соты.

Транскодер участвует в преобразовании данных, передаваемых от подсистемы базовых станций к подсистеме коммутации и наоборот.

Центр управления организует удаленное управление центрами коммутации.

В настоящее время идет постоянное развитие сотовой связи с целью удовлетворения растущих потребностей потребителей. Промежуточным этапом развития сетей СПС стала фаза 2.5G. На этом этапе реализованы конвергентные механизмы, объединяющие потоки передачи речи и данных в рамках одной физической сети. Преимуществом сети GSM/GPRS является возможность выхода во внешнюю глобальную сеть Интернет с АС. Кроме того, она открывает широкие возможности в развитии услуг на базе мультимедийных решений (MMS) [51].

Расширение базовой структуры сети до сети с пакетной передачей данных приводит к естественному увеличению функциональных узлов и, как следствие, к усложнению самой структуры сети.

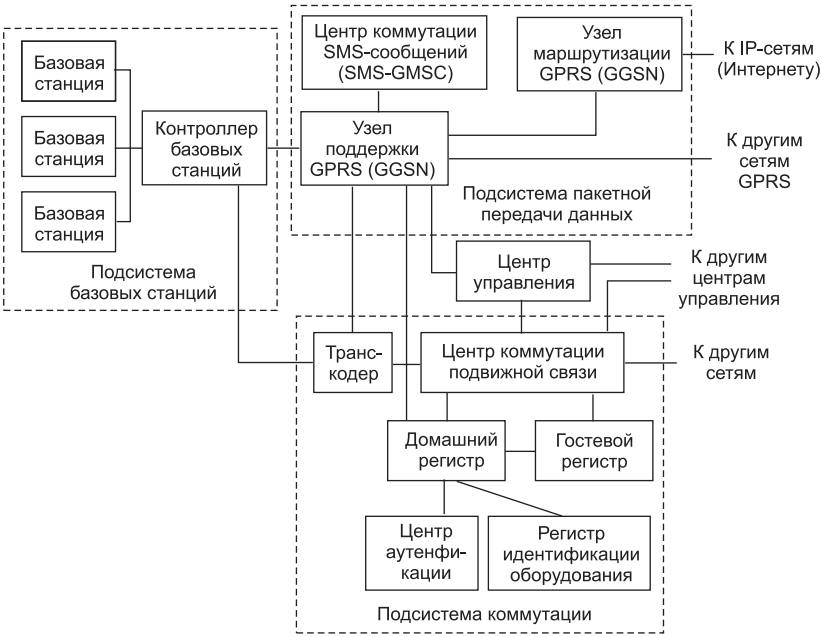


Рис. 1.46. Структурная схема СПС стандарта GSM с реализацией функций пакетной передачи данных

Подсистема GPRS надстраивается над базовой архитектурой сети GSM, как это показано на рис. 1.46. Поскольку существует достаточно явное разграничение подсистем, то нет необходимости говорить об изменении базовой сети, а все работы по внедрению пакетной передачи данных связаны, если можно так сказать, с расширением возможностей базовой сети сотовой подвижной связи стандарта GSM. С этой целью в структуру сети вводятся два основных компонента: узел поддержки и узел маршрутизации (рис. 1.46).

Узел маршрутизации предназначен для отправки и маршрутизации пакетов данных между АС и внешними сетями. Количество таких узлов внутри сети может быть различным, все зависит от архитектуры построения и нагрузки на сеть. Узел маршрутизации обеспечивает взаимодействие сети GPRS и внешними сетями пакетной передачи данных. В узле маршрутизации выполняется преобразование пакетов, исходящих от узла обслуживания, в пакетный протокол передачи данных (например, X.25 или IP).

Узел обслуживания предназначен для отправки пакетов данных АС внутри области обслуживания. Он обеспечивает взаимодействие АС и подсистемы коммутации узлом маршрутизации. К основным его задачам можно отнести передачу и маршрутизацию пакетов; управ-

ление мобильностью; управление логическими каналами; аутентификацию мобильной станции.

Однако введением только физических узлов в сеть GSM изменения не ограничиваются. Для обеспечения полноценной работы подсистемы GPRS необходимо было ввести и новые протоколы передачи данных внутри сети и протоколы взаимодействия с подсистемой коммутации. Для этого в GPRS введены новые радиоканалы, распределение которых является более гибким по сравнению с предыдущими фазами развития протокола GSM (происходит разделение физического канала на логические каналы речи и данных, при этом приоритет отдается речевой информации).

Технология GPRS поддерживает приложения, основанные на стандартных протоколах передачи данных, и осуществляет межсетевое взаимодействие с IP-сетями и сетями, основанными на протоколе X.25. Кроме того, технология GPRS поддерживает все виды основного обслуживания и телесервиса, включая передачу SMS.

Говоря об эффективности использования сети GPRS для передачи данных, можно утверждать, что с меньшими задержками передается информация в случаях:

- пакетной не периодической передачи данных;
- частой передачи небольшого объема данных;
- не частой передачи больших объемов данных.

В технологии GPRS используется пакетный режим передачи как высокоскоростных, так и низкоскоростных потоков данных, а также сигнальной информации.

Технология GPRS оптимизирует использование ресурсов сети и радиоканалов. Существует строгое разграничение между подсистемой радиодоступа и сетевой подсистемой, что дает возможность сетевой подсистеме в дальнейшем использовать другие технологии радиодоступа.

Дальнейшее развитие сетей GPRS ведется в направлении технологии EDGE. Уже сегодня она внедряется крупными операторами с целью повышения пропускной способности каналов передачи данных и увеличения скорости доступа к ресурсам IP-сетей со стороны мобильных станций [51].

В сетях GSM/GPRS реализуются следующие типы интерфейсов:

- интерфейсы взаимодействия с внешними сетями;
- внутренние интерфейсы;
- интерфейс подключения внешнего оборудования;
- интерфейсы подсистемы GPRS.

Рассмотрение структуры сети СПС стандарта GSM позволяет сделать вывод о том, что в ней циркулируют два вида информации:

- информация пользователя (абонента). Объем и степень конфиденциальности информации пользователя могут быть различными. Считается, что пользователь использует сеть СПС для бытовых целей и поэтому последствия от потери информации могут быть незначительными;
- информация управления, определяющая режимы работы оборудования сети СПС и обработки и хранения информации пользователя. Объем информации управления большой, степень конфиденциальности высокая. Последствия неправильного функционирования сети СПС стандарта GSM из-за искажения (потери) этой информации могут привести к потере или искажению информации пользователя [51].

Для защиты от ошибок в радиоканалах подвижной связи GSM используются сверточное и блочное кодирование с перемежением. *Перемежение* обеспечивает преобразование пакетов ошибок в одиночные. *Блочное кодирование* используется для обнаружения нескорректированных ошибок.

Сверточные коды (СК) относятся к классу непрерывных помехоустойчивых кодов. Одной из основных характеристик СК является величина K, которая называется *длиной кодового ограничения*. Она показывает, на какое максимальное число выходных символов влияет данный информационный символ. Так как сложность декодирования СК по наиболее выгодному, с точки зрения реализации, алгоритму Витерби возрастает экспоненциально с увеличением длины кодового ограничения, то типовые значения K малы и лежат в интервале 3...10.

Другой недостаток СК заключается в том, что они не могут обнаруживать ошибки. Поэтому в стандарте GSM для внешнего обнаружения ошибок используется блочный код на основе сверточного кода (2, 1, 5) со скоростью $r = 1/2$.

Наибольший выигрыш СК обеспечивает только при одиночных (случайных) ошибках в канале. В каналах с замираниями, что имеет место в GSM, необходимо использовать СК совместно с перемежением.

В GSM PLMN основные свойства речевых каналов и каналов управления значительно отличались друг от друга. Для речевых каналов необходима связь в реальном времени с короткими задержками при сравнительно низких требованиях к вероятности ошибки в канале. Для каналов управления требуется абсолютная целостность данных и обнаружения ошибок, но допускается более длительное время передачи и задержки.

В речевых и каналах управления используются различные сверточные коды, поскольку скорости передачи и требования по защите

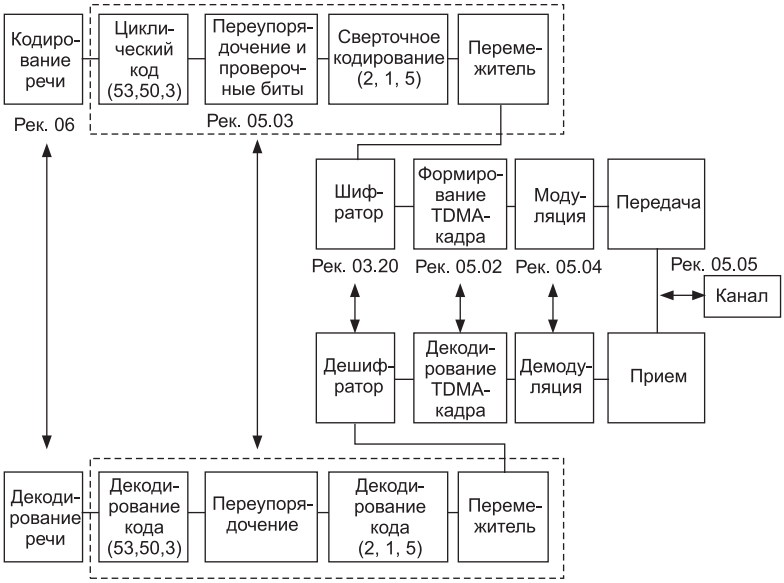


Рис. 1.47. Радиотракт с блоками канального кодирования и перемежения

от ошибок также различны. Для упрощения механизмов кодирования и декодирования для формирования кодов используются только несколько полиномов. Это позволяет использовать сверточный код с одной скоростью $r = 1/2$. Однако, чтобы выполнить требования формирования полноскоростного канала связи, а также привести в соответствие структуру размещения битов со структурой кадров, необходима скорость $r = 244/456 = 0{,}535$. Для выравнивания скорости в речевом канале до $r = 1/2$ применяют прореживание, т. е. периодический пропуск некоторых кодированных символов. Такая операция называется *перфорированием,* а формируемые таким образом коды называются *перфорированными.*

Структурная схема радиотракта с блоками канального кодирования и перемежения, которая соответствует элементам системы и рекомендациям стандарта GSM, показана на рис. 1.47.

В настоящее время все большее распространение получили сети третьего и четвертого поколения, в которых реализованы физические принципы передачи данных — мультидоступ с кодовым разделением каналов (CDMA), в основе которого лежит кодовое разделение канала.

Принцип CDMA заключается в расширении спектра исходного информационного сигнала (в нашем случае речевого). Информационный сигнал может реализовываться двумя различными методами, которые называются «скачки по частоте» и «прямая последовательность» [51].

Скачки по частоте (FH) реализуются следующим образом: несущая частота в передатчике постоянно меняет свое значение в некоторых заданных пределах по псевдослучайному закону (коду), индивидуальному для каждого разговорного канала, через сравнительно небольшие интервалы времени. Приемник системы ведет себя аналогично, изменяя частоту гетеродина по точно такому же алгоритму, обеспечивая выделение и дальнейшую обработку только нужного канала. С помощью FH сейчас пытаются улучшить технические характеристики узкополосных цифровых систем сотовой связи, в частности GSM.

Метод прямой последовательности (DS) основан на использовании шумоподобных сигналов и применяется в большинстве работающих и перспективных системах CDMA. Он предусматривает модуляцию информационного сигнала каждого абонента единственным и уникальным в своем роде псевдослучайным шумоподобным сигналом (он-то и является в данном случае кодом), который расширяет спектр исходного информационного сигнала. (Тут сразу следует отметить, что число вариантов таких кодов достигает нескольких миллиардов, что позволило бы создать персональную связь в масштабах нашей планеты.) В результате проведения описываемого процесса узкополосный информационный сигнал каждого пользователя расширяется во всю ширину частотного спектра, выделенного для пользователей сети (база сигнала при этом становится много больше). В приемнике сигнал восстанавливается с помощью идентичного кода, в результате чего восстанавливается исходный информационный сигнал. В то же время сигналы остальных пользователей для данного приемника продолжают оставаться расширенными и воспринимаются им лишь как «белый шум», который является наиболее «мягкой» помехой, в наименьшей степени мешающей нормальной работе приемника.

При этом обеспечивается высокая степень защиты от активных и пассивных помех, что позволяет работать при низких значениях отношения сигнал/шум (3...5 дБ) со значительно меньшей мощностью передаваемого сигнала. Таким образом, в одном и том же радиочастотном канале одновременно передаются информационные сигналы большой группы пользователей.

Следует также сказать, что CDMA не зря широко используется в военных системах связи, поскольку расширение спектра сигналов позволяет противодействовать преднамеренным искусственным помехам. Если расширить базу радиосигнала до очень больших величин, то можно сделать его уровень ниже уровня шумов. В результате потенциальный противник сможет наблюдать только шумы.

На приемной стороне исходный сигнал восстанавливается.

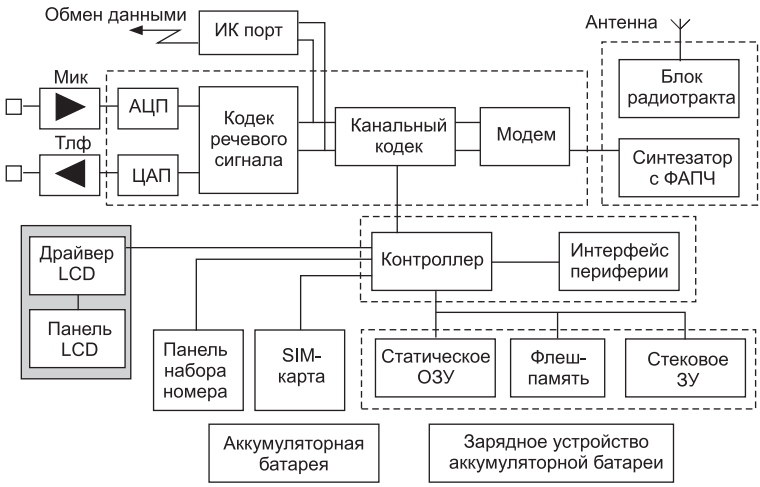


Рис. 1.48. Структурная схема типового образца абонентской станции

Целью разработки стандарта CDMA являлось увеличение емкости системы сотовой связи по сравнению с аналоговой не менее, чем на порядок, и, соответственно, увеличение эффективности использования выделенного спектра частот.

Мобильные абонентские станции. В зависимости от выходной мощности передающих устройств они подразделяются на пять классов в стандарте GSM-900 и два класса в стандарте GSM-1800.

В состав сотового телефона входят аналого-цифровой (АЦП) и цифро-аналоговый (ЦАП) преобразователи речевого сигнала, кодек речевого сигнала, канальный кодек, модулятор-демодулятор (модем), синтезатор частоты с ФАПЧ и собственно радиотракт. Работой узлов трактов приема и передачи, а также устройством индикации управляет контроллер. Кроме того, он коммутирует периферийные устройства. На рис. 1.48 представлена структурная схема типового образца абонентской станции.

Принцип обработки речевого сигнала в системе GSM отображен на рис. 1.49. С микрофона речевой сигнал поступает в тракт передачи. Там он на первом этапе сегментируется в интервалы, а затем преобразуется в цифровой поток со скоростью 13 кбит/с (260 битов на сегмент). Речь кодируется по специальному алгоритму LCP-LTP-RPE-кодирования. На втором этапе для безошибочной передачи цифрового кода и исправления ошибок при приеме осуществляется канальное кодирование. Оно обеспечивает надежную связь при потере не более 12,5 % передаваемой информации. При перемежении производится распределение битов сегмента между восемью пакетами для борьбы с быстрыми замираниями, приводящими к появлению

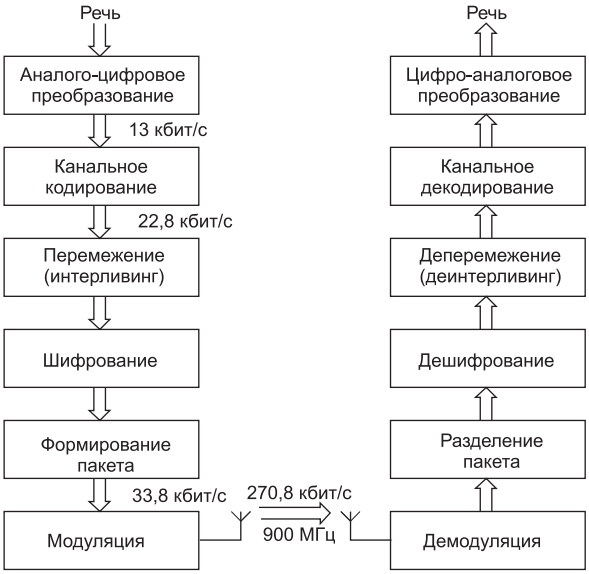


Рис. 1.49. Принцип обработки речевого сигнала в системе GSM

групповых ошибок. После шифрования производится окончательное формирование пакетов, в которые включаются дополнительные биты управления и синхронизации. Сформированные пакеты подаются на модулятор и формирователь радиосигнала.

Для поддержки технологии GPRS разработаны АС (MS — Mobile Station) трех различных классов: «A», «B» и «C». Класс «A» поддерживает как GPRS, так и GSM. Класс «B» поддерживает одновременную работу режимов мониторинга GPRS и обслуживания GSM и наоборот, но полноценная работа возможна при этом только в одном из указанных режимов. Класс «C» поддерживает работу только в режиме GPRS. Абонентские станции должны взаимодействовать с сетями X.25 на основе стандартных протоколов X.3, X.28, X.29 для асинхронного доступа и на основе X.25 для синхронного доступа.

В общем виде временная диаграмма процесса передачи выглядит следующим образом: осуществляется преобразование аналогового речевого сигнала в цифровую последовательность, далее из нее формируется пакет. Все пакеты передаются в рамках временного (TDMA) кадра. Всего в стандарте GSM 900 используются 124 частоты, каждая из которых позволяет передавать до восьми речевых каналов. Реально по некоторым из этих каналов могут передаваться сигналы управления [51].

Абонентские устройства с использованием технологии Bluetooth. В настоящее время технология Bluetooth является твердо устоявшим-

ся коммуникационным стандартом для беспроводной связи на малых расстояниях. Она заменяет целую кучу отдельных кабелей, присоединяющих одно устройство к другому, посредством одной универсальной радиолинии с малым радиусом действия. Например, радиотехнология Bluetooth, встроенная и в сотовый телефон, и в ноутбук, заменяет кабель, используемый в настоящее время для присоединения ноутбука к сотовому телефону. Радиотехнология Bluetooth также обеспечивает универсальный мост к существующим сетям передачи данных, интерфейсу периферийных устройств и, кроме того, обеспечивает механизм для формирования небольших частных специальных групп соединяемых устройств вне инфраструктуры фиксированной сети.

Целью создания технологии было обеспечение надежного сервиса для мобильных абонентов и бизнес-пользователей в рамках компактной радиотехнологии, действующей на малых расстояниях. Данную технологию предполагалось интегрировать в ряд модельных линий широкого диапазона различных устройств. Цель состояла в том, чтобы технология соответствовала таким спецификациям, которые оптимизируют пользование всеми мобильными компьютерными и коммуникационными устройствами, а также обеспечивают использование по всему миру; работу с речью и передачей данных; возможность установки соединений для специальных целей; возможность противостоять помехам от других источников в открытой полосе; очень компактный размер для обеспечения удобной интеграции с различными устройствами; ничтожное энергопотребление в сравнении с другими устройствами, предназначенными для подобных целей; открытый интерфейсный стандарт; низкую стоимость.

Технология Bluetooth имеет следующие характеристики:

- скорость передачи/приема 1 Мбит/с при использовании канала с максимально возможной шириной полосы;
- быстрые переключения частоты во избежание интерференции;
- адаптивная выходная мощность для минимизации помех;
- короткие пакеты данных для минимизации мощности во время помех;
- быстрое опознавание (подтверждение);
- голосовое CVSD (Continuous Variable Slope Delta Modulation)-кодирование, которое дает возможность работы с высокими частотами ошибок по битам;
- гибкие типы пакетов, поддерживающие широкий спектр приложений;
- ненапряженный «бюджет связи», поддерживающий недорогую интеграцию отдельных элементарных сигналов;
- интерфейс передачи/приема, специально приспособленный для минимизации энергопотребления.

Благодаря таким свойствам технология Bluetooth может обеспечивать чрезвычайно гибкую связь с высокими скоростями передачи данных даже при наличии серьезных помех. При заведомо хорошем приеме в благоприятных условиях передачи сигнала по мере усиления помех снижжение качества передаваемого сигнала будет оставаться минимальным и постепенным, что дает возможность сохранения стабильной связи.

Bluetooth имеет RF (Radio Freguency) спецификации для передачи речи и данных на короткие расстояния «точка – мультиточка». Устройство Bluetooth может передавать сигнал через твердые неметаллические объекты. Его номинальный диапазон находится в пределах от 10 см до 10 м, но может быть расширен до 100 м за счет увеличения мощности передаваемого сигнала. Этот эффект, основанный на радиосвязи в коротком диапазоне, облегчает создание специальных соединений для стационарного и мобильного коммуникационного окружения [51].

Принцип передачи информации такими устройствами основан на излучении в эфир радиосигнала. Согласно российскому законодательству каждый оператор системы сотовой связи должен использовать определенный диапазон частот. В современных системах сотовой связи применяются различные способы защиты передаваемой информации и используются различные алгоритмы. Однако применение специальных алгоритмов шифрования, например A5/1 в системе GSM, тоже не гарантирует защиту.

В начале 2000 года было официально сообщено о том, что два известных криптографа Ади Шамир и Алекс Бирюков из Института Вейцмана (Израиль) смогли взломать этот алгоритм шифрования.

Для перехвата разговоров, ведущихся с использованием телефонов сотовой связи, используются специальные комплексы перехвата систем сотовой связи.

Современные комплексы перехвата систем сотовой связи могут обеспечить (в зависимости от конфигурации) слежение за управляющими (вызывными) каналами до 21 соты одновременно, позволяют контролировать и регистрировать телефонные разговоры 10 и более выбранных абонементов.

Комплексы выпускаются в трех видах: «карманном» (в виде сотового телефона), мобильном (в виде компактного блока, ПЭВМ типа Notebook и антенны) и стационарном (в виде настольного блока).

Кроме регистрации контролируемых переговоров комплексы могут комплектоваться (в зависимости от стандарта) некоторыми дополнительными функциями: контроля переговоров по заданному номеру, «сканирования» телефонов и перехвата входящей связи контролируемого абонента.

Для «карманного» варианта возможен контроль разговоров одного абонента в зоне действия соты; для мобильного — одновременный контроль и запись переговоров одного (нескольких) абонентов в зоне действия нескольких сот и возможно ведение базы данных по наблюдаемым сотам; для стационарного варианта возможен одновременный контроль и запись переговоров более десяти абонентов во всей сотовой сети и ведение расширенной базы данных.

Функция «сканирования» телефонов используется для скрытого определения телефонного номера и служебных параметров какого-либо телефона [119].

В случае использования функции перехвата входящей связи контролируемого телефона возможен перехват всех входящих звонков заданного абонента. Основные функции комплекса:

- декодирование служебного канала для выявления номера мобильного телефона, по которому ведется разговор;
- прослушивание непосредственно телефонного разговора;
- возможность одновременного контроля по частоте базовой станции и частоте мобильной трубки, т. е. обеспечение стабильной слышимости обоих собеседников;
- возможность одновременного контроля как по входящим, так и по исходящим звонкам;
- слежение за изменением частоты и сопровождение разговора при переезде абонента из соты в соту;
- контроль нескольких сот из одной точки;
- запись телефонных переговоров с помощью звукозаписывающей аппаратуры в автоматическом режиме;
- фиксация на жестком диске номеров мобильных телефонов, производивших переговоры во всей системе сотовой связи с указанием даты и времени.

На мониторе в процессе работы комплекса отображаются:

- номера всех телефонов, вызываемых по всем сотам системы;
- номера телефонов, вышедших на связь в соте, на которую настроен канал контроля, а также служебная информация.

Программно-аппаратные комплексы используются также для перехвата пейджинговых сообщений. В состав типового комплекса входят:

- доработанный сканирующий приемник;
- ПЭВМ с устройством преобразования входного сигнала;
- программное обеспечение.

Комплекс позволяет решать следующие основные задачи:

- осуществлять прием и декодирование текстовых и цифровых сообщений, передаваемых в системах радиопейджинговой связи,

сохранять все принятые сообщения на жестком диске в архивном файле;

- производить фильтрацию общего потока сообщений, выделение данных, адресованных одному или ряду конкретных абонентов по априорно известным или экспериментально определенным кепкодам, оперативное изменение параметров списка наблюдаемых абонентов;
- осуществлять русификацию всего входного потока сообщений или адресованных только конкретным абонентам, включаемым в список наблюдаемых;
- производить обработку файлов выходных данных в любом текстовом редакторе с реализацией стандартной функции поиска по введенной строке символов и печатью необходимых данных на принтере.

В процессе работы программы на экране отображаются:

- принимаемые по одному из активных каналов сообщения (номер отображаемого канала вводится оператором с клавиатуры без прерывания работы программы);
- текущее время суток и дата;
- время и дата приема каждого отобранного сообщения, его порядковый номер, а также идентификатор соответствующего признака отбора [123].

Для декодирования перехваченных сообщений, закрытых аппаратурой засекречивания используются специальные устройства (например, 640-SCRD-INT). Подобные устройства декодируют и восстанавливают с высоким качеством в реальном времени переговоры, закрытые аппаратурой ЗАС [119].

Средства радиоразведки и специальные комплексы перехвата систем сотовой связи находятся на вооружении специальных служб ведущих иностранных государств и обеспечивают перехват и декодирование сообщений, передаваемых с использованием любых систем связи, включая стандарт GSM.

Еще одна опасность — определение местонахождения абонента. Текущее положение может выявляться двумя способами. Первым из них является обычный метод триангуляции (пеленгования), определяющий направление на работающий передатчик из нескольких (обычно трех) точек и дающий засечку местоположения источника радиосигналов. Необходимая для этого аппаратура хорошо разработана, обладает высокой точностью и вполне доступна. Второй метод — через компьютер, предоставляющей связь компании, который постоянно регистрирует, где находится тот или иной абонент в данный момент времени даже в том случае, когда он не ведет никаких разго-

воров (по идентифицирующим служебным сигналам, автоматически передаваемым телефоном на базовую станцию).

Точность определения положения в городе гораздо выше, чем в сельской местности (размер соты в городе около 1 кв. км против 50...70 кв. км на открытой местности). Анализ данных о сеансах связи абонента с различными базовыми станциями позволяет восстановить все перемещения абонента в прошлом. Такие данные автоматически регистрируются в компьютерах компаний, предоставляющих услуги сотовой связи, поскольку оплата этих услуг основана на длительности использования системы связи. В зависимости от фирмы, услугами которой пользуется абонент, эти данные могут храниться от 60 дней до нескольких лет. Проблемы информационных угроз интересам человека, возникающие из-за прослушивания сотового телефона: это его личная безопасность; информация о передвижении человека, встречах, поездках; информация о личных финансах человека; какие покупки и их стоимость; счета в российских и зарубежных банках; личные акции и информация о недвижимости, машинах, долгах, кредитах; пин и телефонные коды к финансовым картам типа VISA, MASTER Card, а также их номера; информация о родственниках, друзьях и сослуживцах; информация о проблемах в семье и на работе; информация о здоровье человека и его близких людей; список лечебных учреждений, где лечится человек; контакты с органами государственной власти; контакты с иностранными партнерами; контакты, которые в той или иной степени могут скомпрометировать человека; информация о кодах доступа в личный персональный компьютер, в квартиру, коттеджи, которые находятся под сигнализацией; информация о работе и учебе человека; где работает, причины увольнения или перехода на другую работу.

Современные средства связи — мобильные телефонные аппараты — представляют собой многофункциональные устройства. Они способны вести запись аудиоинформации на встроенный микроцифровой диктофон в течение четырех часов и более; хранить в памяти до пятисот фотоснимков, вести с сохранением видеозапись продолжительностью более одного часа; осуществлять передачу по радиоэфиру аудио- и видеоинформации в реальном времени. Кроме того, в них предусмотрена функция «дистанционной активации».

Таким образом, Ваш «надежный друг» может оказать медвежью услугу. Чем «круче» мобильный телефон, тем больше шпионских функций можно задействовать: визуальное фотографирование окружающих лиц и предметов; видеосъемку и акустический контроль в радиусе до 10 метров от мобильного телефона с последующей регистрацией всех говорящих; прослушивание всех входящих и исходящих телефонных разговоров, СМС и электронной почты и

скрупулезная архивация всей информации; четко определять местоположение объекта (мобильника) с точностью до несколько метров; дистанционное включение микрофона с расстояния в десятки тысяч километров; дистанционное прослушивание разговоров через микрофон телефона, даже если основная батарея вынута (для современных смарт-телефонов).

При развитии технологии мобильной связи и появлением смарт телефонов и коммуникаторов, соединяющих функции телефона и компьютера, реализация «специальных» функций или, как их называют, «полицейских» легла и на операционные системы, которые используются в мобильных технологиях. Все труднее стало производить универсальные высокоскоростные, мало потребляющие процессоры для мобильных телефонов, которые реализуют еще дополнительную «полицейскую» функцию. К сожалению, такое значительное перераспределение специальных функций с аппаратной части на программную привела к тому, что опытные программисты стали ловко использовать программную часть. На её базе они создали целый ряд так называемых «spy» (шпионских) телефонов на базе серийно выпускаемых мобильных телефонов.

Еще раз отметим наиболее характерные «тактические возможности» сотового телефона. Помимо общеизвестной миниатюрности, сотовый телефон можно рассматривать как высококачественное подслушивающее радиоустройство. С помощью его можно:

- собирать акустическую информацию на достаточно большом расстоянии (до 5 метров). Эта характеристика у сотового телефона приближается к соответствующей характеристике специальных технических средств;
- активизировать сотовый телефон практически с любого телефонного аппарата. Для специалиста в области информационной безопасности эта характеристика означает наличие у сотового телефона возможности дистанционного управления и, соответственно, приведение в действие телефонной аппаратуры в любой момент времени.

Таким образом, в современных условиях дорогостоящие предварительные проверки помещений на наличие подслушивающей аппаратуры и технических каналов утечки информации, предшествующие обсуждению в этих помещениях конфиденциальных вопросов, теряют смысл в случае проноса аппаратуры несанкционированного получения информации непосредственно участником переговоров.

1.4.10. Основные направления защиты информации от закладочных устройств

Организация и методика проведения работ по технической защите информации будет рассмотрена в третьей главе. А в данной главе

целесообразно сделать общий анализ направлений защиты от закладочных устройств и прежде всего обратить особое внимание на защиту от утечки информации по так называемым «легальным каналам утечки», которые образуются при использовании сотовых телефонов и диктофонов.

Проблема защиты от съема информации с помощью диктофонов до сих пор остается наиболее острой и актуальной и пока далекой от решения. Современные подавители диктофонов не могут решить стоящие перед ними задачи во всех условиях. В определенных условиях они обеспечивают подавление аналоговых и неэкранированных цифровых диктофонов. Наиболее остро стоит проблема с подавлением цифровых малоформатных диктофонов в металлическом корпусе.

Вопрос подавления излучения сотовых телефонов в большинстве случаев решен положительно. Разработано и внедрено большое количество подавителей сотовых телефонов с различными видами подавления, от постоянного излучения до интеллектуального избирательного подавления только излучающих телефонов. Появление различных стандартов сотовой связи и подключение различных радиоинтерфейсов (Bluetooth, Wi-Fi, ZigBee) привело к необходимости обеспечения комплексной защиты. Широкое внедрение в повседневную деятельность сотовой связи привело к острой необходимости решения проблемы определения легальности источников излучения в диапазоне работы сотовой связи. Для разрешения данной проблемы в настоящее время разработаны программно-аппаратные комплексы «Цифра», «Зодиак», МАиС.

Автоматизированный комплекс выявления и идентификации электронных устройств беспроводной связи «Цифра» (рис. 1.50) разработан специально для решения задач специальных проверок технических средств и специальных обследований помещений на наличие устройств несанкционированного получения информации. Комплекс используется для исследований каналов наиболее распространенных беспроводных интерфейсов на наличие признаков несанкционированной передачи информации. Комплекс позволяет оперативно выявлять сигналы устройств несанкционированной передачи информации в сетях GMS, DECT, Wi-Fi, Bluetooth, ZigBee и локализовывать места установки таких устройств в помещении.

Рис. 1.50. Автоматизированный комплекс «Цифра»

Комплекс позволяет оператору проводить одновременный мониторинг как на уровне радиоинтерфейса, так и на MAC-уровне, и поэтому не имеет «слепых» зон, которые свойственны другим комплексам, ориентированным только на один уровень мониторинга. Приемник комплекса, в отличие от обычных комплексов радиоконтроля, специально разработан и оптимизирован под прием и обработку сигналов беспроводных интерфейсов. В комплексе реализована возможность распознавания «свой-чужой» для сигналов различных беспроводных интерфейсов методом сравнения с эталонными образами сигналов из эталонной базы данных. «Цифра» полностью заменяет широкий спектр узкоспециализированных инструментов, средств мониторинга и анализа сетей, активного и пассивного обнаружения беспроводных устройств различных производителей. Комплекс объединяет все современные технологии мониторинга беспроводных устройств в едином пользовательском интерфейсе.

Единая база данных устройств обнаруженных в различных режимах работы значительно повышает производительность работы комплекса. Вся собранная в процессе работы информация структурируется в виде единого отчета установленной формы. В режиме мониторинга базовых станций комплекс может обнаруживать факт применения активных систем перехвата GSM в непосредственной близости от проверяемого объекта. Методическое обеспечение комплекса позволяет оператору проводить работы в соответствие действующими нормативно-методическими документами по спецпроверкам технических средств и спецобследованиям помещений. Функциональные возможности комплекса обеспечивают поиск и обнаружение сигналов GSM 900/1800, DECT, Wi-Fi 2.4/5ГГц, ZigBee Pro 2.4ГГц (802.15.1); панорамный обзор полос контролируемых систем связи; спектральный анализ принимаемых сигналов; автоматизированную оценку параметров сигналов (центральную частоту канала, ширину спектра, уровень); сохранение реализаций принимаемых сигналов в базе данных; поддержание базы данных спектральных эталонов типовых беспроводных интерфейсов; различные варианты отображения спектра (панорама), водопад; цифровой анализ базовых станций GSM с перспективным расширением 3G, 4G; контроль параметров базовых станций GSM (CELL ID, LAC, RSSI, имя оператора). Кроме того комплекс позволяет выполнять цифровой анализ беспроводных интерфейсов: Wi-Fi (IEEE 802.11 a/b/g/n), Bluetooth (IEEE 802.15.1), ZigBee (802.15.4); контроль параметров беспроводных устройств (MAC-адрес (EUI), SSID (EPID), тип устройства, RSSI); активное обнаружение абонентских терминалов GSM с мощностью воздействия не менее 1 Вт; активное обнаружение абонентских терминалов GSM с мощностью воздействия излучения не менее 1 Вт; опция повышения мощности

сигнала генератора активного обнаружения; применение многофункциональных фильтров для оптимизации отображения результатов контроля; установка определяемых пользователем реакций на возникающие события; формирование общего отчета по результатам работы; опция дистанционного управления комплексом.

Комплекс постоянно модернизируются под новые стандарты передачи информации и изменения в нормативных документах, база эталонных образов регулярно обновляется производителем. Развертывание в организациях Wi-Fi-сетей для обмена информацией внутри организации привело к тому, что Wi-Fi-сети могут использоваться устройствами несанкционированного получения информации в качестве канала передачи по целому ряду причин:

- сигналы Wi-Fi-устройств имеют достаточно сложную структуру и широкий спектр, поэтому они не поддаются идентификации обычными средствами радиомониторинга;
- практически на каждом объекте или вблизи него развернуты Wi-Fi-сети (частные или общего пользования), при этом крайне сложно отличить легальных клиентов от клиентов с возможностями негласного получения информации. Это позволяет эффективно маскировать несанкционированную передачу информации среди легальных Wi-Fi-каналов;
- в крупных городах сети Wi-Fi общего пользования имеют зону покрытия достаточную, чтобы гарантировать возможность подключения к ним устройств с возможностями негласного получения информации;
- ресурсы, которые предоставляют каналы Wi-Fi-сетей, позволяют передавать звук, данные, видео в реальном времени, при этом практически все Wi-Fi-сети имеют высокоскоростной доступ в Интернет.

Кроме того, в настоящее время продаются малогабаритные Wi-Fi-устройства, позволяющие передавать данные, речевую или видеоинформацию, например беспроводные Wi-Fi-видеокамеры, которые легко могут быть переделаны для использования в качестве устройств негласного получения информации. Модернизация Wi-Fi-устройств на уровне драйвера позволяет сделать их практически невидимым для большинства штатных программ управления и мониторинга Wi-Fi-сетей. Использование специальных программ мониторинга трафика Wi-Fi также является неэффективным для поиска устройств негласного получения информации. Устройства негласного получения информации, как правило, являются абсолютно легальными с точки зрения администрирования сетей, и попытки поиска их средствами поиска нелегальных возможностей не эффективны.

Рис. 1.51. Комплекс «Зодиак»

Комплекс «Зодиак» (рис. 1.51) разработан как специализированный инструмент автоматизированного контроля канала утечки информации по Wi-Fi-сетям.

Комплекс «Зодиак» принимает и анализирует пакеты данных, передаваемые все устройствами Wi-Fi в зоне радиовидимости. На основе полученной информации «Зодиак» составляет список активных Wi-Fi-устройств и их параметров. Представление информации о структуре сетей реализовано в виде взаимосвязанных деревьев устройств и их связей. Это позволяет в реальном времени отслеживать появление новых устройств или соединений. Анализ полученных пакетов позволяет обнаруживать клиентов сетей и точки доступа не только в зоне радиовидимости комплекса, но и за ее пределами. Комплекс в реальном времени контролирует: аппаратный адрес сетевого адаптера (MAC адрес); имя сети (SSIDE) для точек доступа; время обнаружения; уровень активности; количество активных соединений; режим работы устройства; уровень сигнала от устройства.

Мониторинг осуществляется в двух режимах: пассивный мониторинг пакетов (комплекс только принимает и анализирует пакеты); активный поиск, при котором комплекс провоцирует активность «скрытых» клиентов и точки доступа, посылая пакеты специальной формы. В этом режиме комплекс может обнаруживать устройства, невидимые в пассивном режиме. В комплексе реализован мультирежимный доступ — возможность подключения к нескольким доступным сетям, в том числе закрытым (при условии наличия пароля), в качестве клиентов с одновременным анализом пакетов этих сетей.

На основе адресной информации из пакетов для каждого отправителя информации ЗОДИАК позволяет построить в реальном времени структурированное дерево взаимосвязанных с ним получателей, с которыми отправитель обменивается информацией в настоящее время или обменивался ранее. Комплекс позволяет обнаруживать, в том числе, связи с получателями пакетов не являющихся клиентами Wi-Fi-сетей, например клиентами локальных сетей, к которым подключены точки доступа, и клиентов Интернета (http://www.nimrod.ru/spii.jpg).

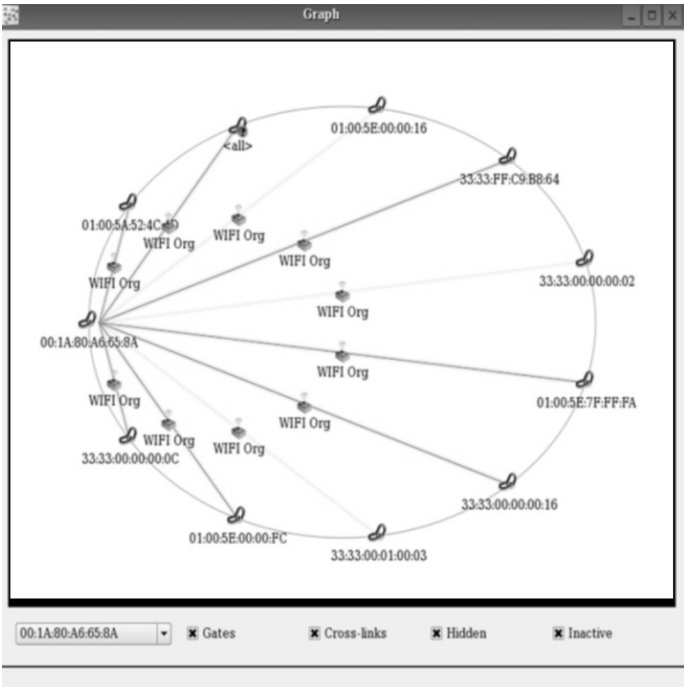


Рис. 1.52. Графическое представление данных

Программа комплекса позволяет контролировать следующие параметры соединений: аппаратный адрес сетевого адаптера получателя (MAC-адрес); аппаратный адрес сетевого адаптера шлюза (MAC-адрес); время первого обнаружения сеанса; время обнаружения текущего сеанса; длительность текущего сеанса; объем передаваемого трафика; уровень активности; протокол соединения; порт; IP-адрес отправителя; IP-адрес получателя.

Для визуализации связей устройства используется графическое представление данных (рис. 1.52).

По окружности графа отображаются все получатели информации от выбранного устройства, а также шлюзы и перекрестные связи получателей. Граф различает активные и неактивные связи, оповещает о появлении новых связей, позволяет отследить ретрансляторы и точки выхода в другие сети, в том числе Интернет. Граф позволяет оперативно отследить появление опасных связей устройств, работающих в штатном режиме.

Круговая диаграмма активности устройства помогает оценить распределение объема трафика, передаваемого с устройства, по получателям и оперативно определить направление, по которому мо-

жет передаваться трафик большого объема (например, видеоинформация).

Временной график активности устройства позволяет оператору отслеживать хронологию передачи трафика и обнаруживать, в какой момент времени устройство начинает и заканчивает сеанс связи. Сопоставляя полученную информацию с расписанием режимных мероприятий на объекте, оператор может обнаруживать незарегистрированные ранее устройства.

Хронометраж трафика по выбранному устройству можно построить и для ранее сохраненных в режиме автоматической регистрации данных, чтобы анализировать информацию историю активности устройства, например во внерабочее время.

Экспертная версия позволяет генерировать отчеты о результатах мониторинга в файл в формате .cvs (поддерживается табличными редакторами MS Excel и OpenOffice Calc).

Для выявления «опасных» сочетаний параметров устройств в комплексе реализован инструмент правил. С их помощью оператор задает «опасные» сочетания параметров устройства, которые будут отслеживаться комплексом в автоматическом режиме. При обнаружении таких параметров комплекс зафиксирует тревогу и выполнит заранее определенные действия. Правила могут использоваться для настройки фильтрации списков устройств и соединений по определенному набору параметров, чтобы оптимизировать представление информации при высокой сетевой активности, например чтобы скрывать неактуальные устройства или связи.

Для локализации клиентов сети Wi-Fi на объектах большой площади или этажности с точностью до 10 м должна быть развернута многозонная конфигурация комплекса. Алгоритм разработан на основе технологии WPS.

Программно-аппаратный комплекс ПАК «МАиС» предназначен для мониторинга состояния базовых станций сотовой связи стандарта GSM и протокола передачи данных Wi-Fi, а также обнаружения ложных базовых станций на контролируемых территориях.

При работе ПАК обеспечивается единство и точность результатов измерений. Результаты измерений одинаковых объектов, проводимых при одинаковых условиях, должны совпадать при их повторении. Комплекс использует индикаторные методики проведения исследований, при которых алгоритм ПАК позволяет провести усреднение и выбраковку результатов, тем самым обеспечивая надлежащее качество измерений.

Комплекс обеспечивает мониторинг следующих параметров:

- параметры сети сотовой связи (состояние мобильной станции и базовой станции);

- параметры смены канала (хэндовер);
- параметры соседних сот;
- параметры службы передачи данных GPRS;
- параметры радиосигнала;
- список частот;
- осуществить привязку местоположения комплекса к цифровой карте;
- статистика соединений;
- механизм обработки статистической информации и генерации отчетов.

  В качестве базовых были выбраны следующие параметры:
- уровень сигнал/помеха (C/I, Carrier to Interference);
- уровни сигналов на входе приемника мобильной станции и на входе приемника базовой станции;
- уровень качества передачи фреймов;
- расстояние от базовой станции до мобильной станции;
- уровень мощности сигналов соседних базовых станций с учетом разрешенных частот (Color Code);
- работоспособность механизма коррекции синхронизации;
- уровень мощности базовой станции;
- уровень мощности мобильной станции.

  Поддержка работы UMTS-модуля в составе комплекса.

  Рассмотрим принцип работы комплекса.

В ПАК устанавливается база сотовых вышек GSM-связи и протокола передачи данных Wi-Fi всех операторов контролируемой зоны, получивших разрешение на их установку, с привязкой к местности.

При включении комплекс регистрируется в сети и анализирует состояние сотовой связи, для чего получает информацию о доступных базовых станциях вокруг себя, определяет принадлежность базовой станции к оператору. Проводит анализ идентификационных и технических данных базовых станций. Оценивает уровни сигналов, поступающих с каждой базовой станции. Затем эти данные обрабатываются и наносятся на предустановленную карту территория покрытия каждой базовой станции операторов (рис. 1.53).

При движении ПАК на карту наносятся местоположения вышек, уровень сигнала, зона покрытия. Одновременно проводится мониторинг средств перехвата сотовой связи стандарта GSM (фейковых вышек).

Определение о ложной (временной) сотовой базе происходит по следующим параметрам:

- определяется присутствие сотовой базы в списке баз операторов и ее идентификация по координатам официальной установки;

Рис. 1.53. Вид дисплея в режиме анализа базовых станций

- по наличию скачкообразного изменения уровня сигнала в данном месте;
- по изменению точки местоположения сотовой базы (ее передвижению).

Анализ состояния радиоинтерфейса Wi-Fi начинается со сбора комплексом информации о наличии в зоне видимости устройств Wi-Fi IEEE 802.11 a/b/g/n. Затем программа комплекса анализирует состояние обнаруженных устройств и выводит на дисплей их список со следующими параметрами:

- расстояние и направление на интересующее нам устройство;
- MAC- и IP-адрес каждого обнаруженного устройства;
- наличие связи данного устройства с клиентом в данный момент и информацию о работе двух клиентов;
- зона покрытия данного устройства на карте с привязкой к направлению.

Кроме того, программное обеспечение комплекса позволяет сохранять в памяти следующие данные:

- технические параметры базовых станций сотовой связи и радиоинтерфейса Wi-Fi;
- передвижение оператора ПАК с построением схем движения на карте и привязкой их к сотовым базам.

Данная информация сохраняется в памяти устройства в качестве историй с привязкой их к дате/времени в графическом виде в формате KML.

В настоящее время разработано огромное количество подавителей излучения работающих сотовых телефонов («легальных ЗУ»).

Рис. 1.54. Общий вид стационарного комплекса

Они отличаются: мощностью (большая, малая, регулируемая); вариантами исполнения (стационарные, мобильные, «карманные»); числом каналов подавления (одноканальные, многоканальные); принципами работы (подавители непрерывного излучения, интеллектуальные подавители) и т. д.

Рассмотрим некоторые из последних разработок в этой области.

Мультистандартный интеллектуальный блокиратор радиоинтерфейсов «АРЕС» является комплексом многоуровневой защиты от утечки информации по каналам сотовой связи стандартов NMT450i, CDMA-2000, DAMPS/TDMA, CDMA-800, GSM-900/1800, DECT, радиоинтерфейсам (Bluetooth, Wi-Fi, ZigBee) и другим радиочастотным каналам. Комплекс состоит из нескольких взаимодополняющих друг друга модулей (рис. 1.54), обеспечивающих:

- сканирование заданного диапазона и постановку прицельных помех на выявленных частотах работающих передатчиков. Критерием принятия решения о постановке помехи является наличие несанкционированного источника радиоизлучения (передатчика). Диапазон частот для сканирования устанавливается заранее (110...113 МГц, 400...450 МГц или др.) и выбирается на основании анализа радиочастотной обстановки в конкретном месте;
- интеллектуальное блокирование каналов сотовой связи стандартов NMT450i, CDMA-2000, DAMPS/TDMA, CDMA-800, GSM-900/1800, DECT. Обеспечивается защита от несанкционированной передачи информации по каналам сотовой телефонии и противодействие использованию сотовой связи в качестве канала управления специальными техническими средствами. При этом излучение блокирующего сигнала минимально и происходит только в момент передачи базовой станцией сигнала конкретному абоненту в зоне блокирования.
- автоматическое блокирование радиоинтерфейсов Bluetooth, Wi-

Рис. 1.55. Пример записи настроек через меню

Fi, ZigBee. Узконаправленная помеха включается только при появлении соответствующего сигнала радиообмена.

Кроме того, комплекс может работать в двух режимах: под управлением ПК и в автономном режиме. При работе под управлением ПК программа управления обеспечивает возможность получения на мониторе визуальной информации о текущей загруженности данного диапазона. Просмотр временной диаграммы загруженности выбранного диапазона, которая отображается в нижней части окна программы, осуществляется левой кнопкой мыши. Розовым цветом подсвечены диапазоны, в которых осуществляется блокирование. Параметры блокирования устанавливаются во вкладке Menu — Blockingsettings. При этом обеспечивается выставление необходимой мощности подавления, регулируемой с шагом 3 дБ и имеющей 8 градаций (0 — блокиратор отключен, 7 — максимальная мощность). Блокирование осуществляется в моменты превышения выставляемого оператором порога (синий маркер на индикаторе, перемещается с помощью мыши). Комплекс может работать от сети и имеет автономное питание от аккумуляторов. Продолжительность работы от аккумуляторов в среднем не менее 4 часов.

При автономной работе используются параметры записанные оператором при настройке комплекса через ПК (рис. 1.55).

Запись настроек производится выбором в меню пункта Save settings to devise. Затем в необходимое окно записываются выбранные параметры подавления. Записанные параметры используются в автономном режиме.

Переносной вариант комплекса «Арес-М» (рис. 1.56) монтируется в корпусе кейса. Имеет автономное питание от аккумуляторов. Продолжительность работы в среднем не менее 4 часов.

Рис. 1.56. Общий вид переносного варианта комплекса

Рис. 1.57. Устройство защиты конфиденциальных переговоров ST 202 UDAV-M

Устройство защиты конфиденциальных переговоров ST 202 UDAV-M (рис. 1.57) предназначено для обеспечения информационной безопасности переговоров за счет санкционированного ограничения работы мобильных телефонов и некоторых цифровых каналов передачи данных (Wi-Fi, Bluetooth, WiMax). Одно изделие способно заблокировать работу мобильных телефонов и цифровых устройств передачи данных, расположенных на расстоянии до 40 метров. Дальность блокирования зависит от расстояния до ближайшей базовой станции мобильной связи.

Устройство имеет 10 независимых каналов, работающих в разных диапазонах. Время работы неограниченно. Встроенные диапазонные антенны обеспечивают необходимый уровень излучения по всем каналам. Максимальная выходная мощность зависит от частоты канала подавления и составляет: для CDMA-450 — 0,8 Вт; для GSM-900 — 2 канала по 1,8 Вт; для GSM-1800, DECT — 2 канала по 1,8 Вт; для 3G — 2 канала по 1,5 Вт; для 3Glow — 1,5 Вт; для Wi-Fi, Bluetooth, WiMax (4G) — 1 Вт.

Принцип действия устройства основан на блокировании служебных сигналов систем связи с помощью постановки заградительной помехи в соответствующем диапазоне частот. Предусмотрена возможность регулировки излучаемой мощности по каждому используемому каналу подавления. Ограничение мощности излучения позволяет сконфигурировать необходимую зону подавления. ST202 может работать в ручном или автоматизированном режиме.

Работа в ручном режиме возможна в двух вариантах:

1) без ограничения радиуса зоны подавления;

2) с конфигурированием необходимой зоны подавления.

Работа с ST 202 в автоматизированном режиме возможна совместно с детектором мобильных устройств цифровой связи ST 062, при подключении релейного выхода ST 062 с помощью кабеля к входу дистанционного управления ST 202.

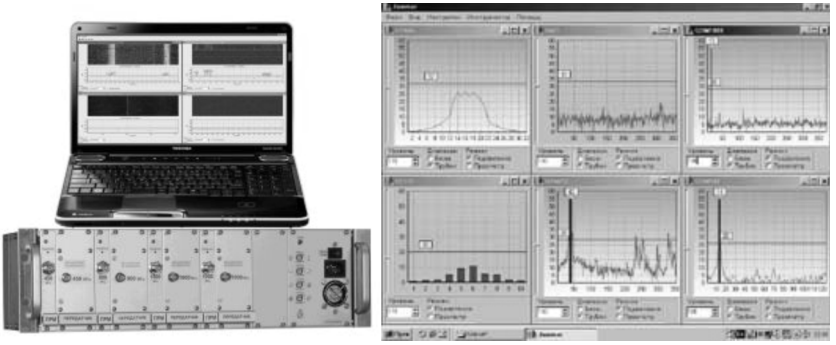


Рис. 1.58. Универсальная аппаратура интеллектуального блокирования сотовой связи RS multijammer

При правильной настройке порога срабатывания детектора излучение работающего мобильного телефона, находящегося в пределах защищаемой зоны, фиксируется индикатором поля ST 062 и подаётся сигнал на его блокирование.

Выход в рабочий режим происходит за время не более 15 секунд, после чего канал связи разрывается. ST 202 излучает блокирующий сигнал в течение 1 минуты, после чего излучение прекращается. В течение 30...35 секунд после выключения помехи, ST 202 находится в пассивном режиме (не управляемом), после чего снова переходит в режим ожидания команды на включение. Данная задержка предусмотрена для восстановления рабочего режима ST 062.

В автоматическом режиме комплекс не рассчитан на блокировку передачи и приема SMS-сообщений, так как сигналы при данном типе связи слишком короткие.

При входе в защищаемую зону с мобильным телефоном в режиме связи некоторое время связь будет сохраняться. Моментальное блокирование при пересечении границы зоны невозможно.

RS multijammer (RS/MJ) (рис. 1.58) — это универсальная аппаратура интеллектуального блокирования сотовой связи и беспроводного доступа любых действующих стандартов внутри заданной зоны, предназначенная для защиты утечки информации по каналам сотовой телефонии, Интернету и беспроводным сетям, а также предотвращающая использование сотовой связи в качестве канала управления, например, взрывными устройствами. Архитектура системы позволяет строить её из отдельных независимых блоков, что чрезвычайно важно при современных темпах развития связи, телефонии, беспроводного доступа и т. д. Кроме того, решение задачи блокирования изначально подразумевает использование системы, распределенной в пространстве, так как в пространстве блокируемой зоны действует множество

базовых станций, точек доступа и прочих радиотерминалов. Контроль диапазонов сотовой связи и беспроводного доступа осуществляется панорамными приемниками. Комплекс реализует направленное блокирование сигнала базы и точек доступа, адресованных конкретному абоненту, предпринимающему попытки установить связь. Блокирующий сигнал имеет импульсную структуру и минимален по мощности. Его воздействие на человека гораздо слабее, чем непосредственно сотового телефона или терминала. Эффективность блокирования контролируется компьютером. Система может быть использована в залах для проведения закрытых совещаний, на секретных предприятиях и военных базах, в учреждениях пенитенциарной системы (зоны, тюрьмы, изоляторы и т. д.), а также для соблюдения тишины в концертных залах, театрах, аудиториях, церквях и т. д.

Система RS/MJ может решать следующие задачи:

- обеспечивает обнаружение включенного абонентского терминала или сотового телефона в момент выхода в эфир его передатчика и оценивает его параметры, а именно: принадлежность к стандарту, номер канала (частоту несущей), уровень сигнала;
- в режиме подавления осуществляет блокирование сигнала базовой станции выявленного дуплексного канала (прямого: база — абонент) на момент передачи информации данному (выявленному) абоненту;
- в автономном режиме (без оператора и управляющего компьютера) выполняет подавление работающих и входящих в связь абонентских терминалов, при этом абонент остается на обслуживании в сети, но сигнал вызова абонента не проходит.

Кроме того, в комплексе предусмотрены: регулировка усиления приемного тракта и порога обнаружения для каждого из стандартов в отдельности, что позволяет регулировать зону блокирования под условия конкретного помещения, при этом имеется возможность сохранения данных настроек; возможность отключения и включение режима блокирования для каждого из стандартов; в режиме обслуживания оператором информация о выходящих в эфир абонентах отображается на дисплее компьютера; во всех режимах работы ведется протоколирование выходов абонентов в контролируемой зоне.

В комплексе также предусмотрено дистанционное управление и работа в компьютерной сети. Аппаратура предназначена для круглосуточной эксплуатации и имеет режим самодиагностики. Радиус действия (зона подавления) аппаратуры не менее 30 метров. Для расширения зоны действия предусмотрены (опционально) дополнительные усилители мощности и система антенных разветвителей и коммутаторов, что позволяет спроектировать систему под конкретные условия эксплуатации.

Рис. 1.59. Подавители семейства «Кокон» и «Ладья»

Архитектура комплекса позволяет компоновать аппаратуру в соответствии с решаемыми задачами.

Возможность использования сотового телефона в режиме радиомикрофона, с негласной активацией без ведома владельца телефона, привело к необходимости разработки и применения индивидуальных средств защиты. В настоящее время такие средства разработаны и предлагаются многими фирмами, но все они имеют практически один и тот же принцип действия. Работу данных устройств рассмотрим на примере подавителей семейства «Кокон» и «Ладья».

В случае негласной дистанционной активации телефона в режим прослушивания единственным демаскирующим признаком является изменение напряженности электромагнитного поля (т. е. передатчик сотового телефона несанкционированно включается на передачу). Это изменение фиксируется индикатором поля, который дает команду на автоматическое включение акустического шумогенератора, расположенного внутри изделий. Уровень акустического шума на входе микрофона трубки сотового телефона таков, что обеспечивается гарантированное закрытие этого канала утечки информации, т. е. зашумляется весь тракт передачи речевой информации таким образом, что на приемном конце отсутствуют какие-либо признаки речи.

Кроме того, последние разработки в этой области решают задачу блокирования режима записи диктофонов, встроенных в сотовые телефоны.

Закладочные устройства являются искусственными (рукотворными) техническими каналами утечки информации, предназначенными для скрытого получения информации, поэтому при их установке предпринимаются меры для маскировки различными способами. Маскировка закладочных устройств существенно затрудняет их поиск и защиту от утечки информации. На практике для защиты объекта от закладочных устройств могут быть использованы различные варианты действий, связанных с такими условиями деятельности объекта, как:

- предшествующие проверки объекта на наличие закладочных устройств;
- необходимость разовых проверок перед проведением конфиденциальных мероприятий;
- обеспечение гарантированной защиты объекта, учитывающей весь спектр возможных действий злоумышленника, и т. п.

Применительно к непосредственным действиям службы безопасности это выливается в такие действия, как:

- обнаружение и противодействие работе закладочных устройств на объекте защиты;
- проведение мероприятий по недопущению установки закладочных устройств на объекте защиты;
- проведение превентивных мероприятий, гарантирующих (с определенной вероятностью), что за счет таких мер, как использование, например, акустического и электромагнитного экранирования или зашумления, даже внедренная закладка не будет эффективной.

Следует отметить, что проведение подобных мероприятий связано, наряду с использованием специальной техники, с широким привлечением систем охранной сигнализации, телевизионных систем наблюдения, контроля за доступом на объект и в его основные помещения и т. п.

Как правило, мероприятия, направленные на нейтрализацию и выявление закладок, проводятся в комплексе с защитой объекта от утечки информации в зависимости от стоящих задач, но так как мероприятия по выявлению и нейтрализации закладок имеют свою специфику, рассмотрим их основные направления.

Мероприятия по недопущению установки закладочных устройств можно условно разделить на организационные и технические.

К организационным мероприятиям относятся: организация работы «защищаемых» помещений на объекте; организация контроля за доступом посетителей и сотрудников; организация контроля работы посетителей и сотрудников; организация проверки помещений объекта, техники, находящейся на нем и в том числе вновь поступающей, на наличие закладочных устройств; анализ методов и способов установки закладочных устройств, их камуфляжа.

К техническим мероприятиям можно отнести: создание системы технических средств охраны; создание системы охранной сигнализации; создание телевизионной системы наблюдения; создание системы контроля управления доступом; использование технических средств, сигнализирующих о подключении в защищаемых помещениях закладочных устройств к линии связи, сети питания и т. п. Использование технических средств контроля на наличие закладочных устройств

в поступающей технике и помещениях: средства контроля радиоизлучений и излучений в линиях связи, питания управления; средства контроля ИК излучений; средства нелинейной и подповерхностной радиолокации; рентгеновские установки.

Мероприятия по обнаружению и противодействию работе закладочных устройств.

Организационные: аналитическая работа по выявлению возможных мест установки закладочных устройств (с учетом особенностей их работы); организация работы службы безопасности по контролю излучений в эфире, сетях связи, управления; анализ частотного диапазона и способов работы закладочных устройств.

Технические можно условно подразделить на мероприятия, связанные с обнаружением закладочных устройств, и мероприятия, направленные на противодействие съему информации с их использованием.

Мероприятия по обнаружению могут включать: контроль сигналов в линиях связи, управления, питания, охранных систем; контроль радиоизлучений в районе объекта; контроль ИК излучений в районе расположения объекта; использование аппаратуры нелинейной радиолокации и подповерхностной локации; использование рентгеновских установок, тепловизионных систем, металлодетекторов; использование технических средств, сигнализирующих о подключении закладочных устройств; использование средств визуального контроля.

Мероприятия по противодействию могут заключаться: в использовании электромагнитных средств зашумления; в использовании акустических шумовых устройств; в отключении (разрушении) закладочных устройств.

Анализ характеристик закладочных устройств позволяет сделать определенные выводы:

1. В комплексе мероприятий по организации защиты объектов от утечки информации существенную роль играют мероприятия по выявлению и нейтрализации или физическому уничтожению закладочных устройств.

2. Поиск и обнаружение закладочных устройств связаны с определенными трудностями, вызванными тем, что закладочные устройства очень тщательно маскируются. Следовательно, необходимо четко представлять демаскирующие признаки, по которым их можно определить.

Как правило, наиболее точно и быстро закладочные устройства определяются в момент их функционирования. К признакам, демаскирующим их работу, можно отнести:

- электромагнитные излучения, возникающие при передаче перехваченной радиозакладками информации в радиодиапазоне;

- передачу перехваченной информации в низкочастотном диапазоне без излучения в эфир;
- передачу перехваченной информации в ИК диапазоне.

При установке закладочных устройств в схемах и устройствах подключения возможны:

- «отсос» энергии из систем питания, управления и связи для питания закладочных устройств;
- изменение характеристик тракта передачи информации при подключении закладочных устройств;
- сам факт подключения, связанный с изменением в линиях передачи информации, связи и управления (например, разрыв линии при установке закладочного устройства).

К визуально обнаруживаемым демаскирующим признакам закладочных устройств относятся действия злоумышленников при их установке. Это связано, прежде всего, с необходимостью проникновения в здания, помещения для установки устройств на стекла окон, несущие конструкции зданий и т. п. Кроме того, возможна такая форма появления закладочных устройств в охраняемых помещениях, как организация «подарков» с вмонтированными закладочными устройствами.

Так как визуальное обнаружение закладочных устройств существенно затруднено, а зачастую, и невозможно (при монтаже закладочных устройств внутри изделий без изменения их основного функционального назначения), то наиболее оптимальным является определение радиозакладочных устройств по их радиоизлучениям.

При использовании злоумышленником радиозакладочных устройств обнаружение их возможно по факту излучения (передачи перехваченной информации). В настоящее время можно встретить радиозакладки, работающие в диапазоне частот от 20 до 3000 МГц и более. Это и определяет требования к диапазону работы приемного устройства, используемого для их поиска.

При определении излучений радиозакладочных устройств можно использовать такие особенности их радиоизлучений, как:

- наличие относительно мощных гармоник, регистрируемых контролирующими супергетеродинными приемниками (в современных радиозакладках ослабление радиоизлучений гармоник более 50 дБ);
- излучения радиозакладок, как правило, проявляются в свободном, не занятом участке диапазона;
- сигнал радиозакладки выделяется при изменении пространственного положения приемной (зондирующей) антенны относительно других сигналов (поляризация);
- спектр излучения радиозакладки, работающей без кодирования, расширяется с увеличением уровня звука;

- если закладка работает без маскировки, то в перехваченном сигнале может прослушиваться шум помещения (или тестового сигнала);
- время работы (излучения) радиозакладок, как правило, совпадает со временем интенсивной работы (обсуждения) конфиденциальных вопросов.

В качестве приемных устройств поиска радиозакладок могут быть использованы:

а) широкополосные приемные устройства;

б) супергетеродинные приемные устройства;

в) аппаратно-программные комплексы.

Для определения местоположения радиозакладочных устройств используются радиопеленгаторные устройства или специальные устройства, позволяющие определить местоположение закладки по сдвигу сигнала, излученного акустическим излучателем и принятым из эфира этого же сигнала, излученного закладкой. Однако, учитывая наличие рефракционных процессов в защищаемых помещениях, за счет сложной картины отражения волн от окружающих предметов интерьера, зачастую, не представляется возможным использовать радиопеленгаторные устройства для обнаружения местоположения закладочных устройств.

Так как для поиска закладочных устройств приходится использовать широкий комплекс специальной аппаратуры, а каждое из рассмотренных выше типов передающих и приемных устройств обладает определенными положительными и отрицательными характеристиками, целесообразно более детально рассмотреть тактико-технические характеристики и функциональные возможности поисковой аппаратуры.

Контрольные вопросы для самостоятельной работы

1. Дайте определение технического канала утечки информации.
2. В чем отличие основных технических средств (ТСПИ) от вспомогательных технических средств и систем (ВТСС)?
3. Дайте определение контролируемой зоны (КЗ).
4. Назовите основные виды каналов утечки информации, обрабатываемой ТСПИ.
5. Объясните физическую сущность возникновения побочных электромагнитных излучений.
6. Какие причины приводят к возникновению электрических каналов утечки информации?
7. Что представляют собой закладочные устройства?
8. Назовите основные виды каналов утечки речевой информации.
9. Как реализуется метод высокочастотного навязывания?
10. На чем основана реализация лазерного канала утечки информации?
11. Как реализуется метод высокочастотного облучения?
12. Назовите основные виды каналов утечки информации, передаваемой по каналам связи.

13. Назовите способы получения видовой информации.

14. Перечислите принципы организации несанкционированного доступа к информации, обрабатываемой средствами вычислительной техники.

15. Что представляет собой программная закладка?

16. К каким последствиям может привести использование программной закладки?

17. Какие каналы утечки информации могут возникать при работе средств вычислительной техники?

18. Какие излучения относятся к электромагнитным каналам утечки информации?

19. За счет чего возникают электрические каналы утечки информации?

20. Каким параметром определяется зона возможного перехвата информации?

21. Каковы основные акустические параметры речевых сигналов?

22. От чего зависит звукоизоляция основных строительных конструкций?

23. Что является наиболее распространенными причинами снижения звукоизоляции строительных конструкций?

24. Какие элементы строительных конструкций наиболее опасны с точки зрения несанкционированного съема информации?

25. Какие основные задачи необходимо решить для обнаружения записывающих диктофонов?

26. Назовите основные виды и источники излучения в различных типах диктофонов.

27. Какие различия в расположении сот в городской и сельской местности?

28. Назовите основные стандарты аналоговой и цифровой сотовой связи.

29. Каким образом осуществляется коммутация между основными элементами сотового комплекса?

30. Назовите функции сотового телефона, которые можно использовать для несанкционированного получения информации.

31. Какие принципы заложены в программно-аппаратный комплекс «Цифра»?

32. Назовите назначение и основные функции комплекса «Зодиак».

2 СРЕДСТВА ОБНАРУЖЕНИЯ КАНАЛОВ УТЕЧКИ ИНФОРМАЦИИ

В предыдущей главе были рассмотрены возможные каналы утечки информации, основной объем из которых составляют технические каналы. В свою очередь, большую часть из них представляют каналы, получающие информацию, переносимую тем или иным видом промодулированного электромагнитного сигнала. Для передачи сигнала обязательно должно иметься передающее устройство (передатчик) того или иного вида. Одним из основных признаков наличия нелегального передатчика являются незарегистрированные радиоизлучения. Поэтому в арсенале средств обеспечения информационной безопасности важное место занимают устройства, предназначенные для обнаружения средств несанкционированной передачи информации за пределы контролируемой зоны по радиоканалу.

Речевая информация, циркулирующая в помещении, может негласно транслироваться за его пределы при помощи специальных электронных устройств — акустических закладок. Наиболее широко распространены акустические закладки, передающие информацию по радиоканалу и использующие в качестве чувствительных элементов микрофоны или датчики акселерометрического типа (радиостетоскопы).

Электропитание акустических закладок осуществляется от автономных источников, электросети, телефонной линии или от источников питания приборов, в которые они устанавливаются. Радиозакладки с автономным источником электропитания имеют мощность, не превышающую, как правило, 10 мВт, и дальность передачи информации от 100 до 200 м. Встречаются образцы мощностью в несколько десятков мВт и дальностью действия до 1000 м. Мощность излучения радиозакладок, питающихся от бортовой или электросети, может составлять порядка 100 мВт, что обеспечивает дальность передачи примерно 2...8 км.

Наиболее часто радиозакладки работают в метровом, дециметровом и СВЧ диапазонах, на частотах 24...28, 64...70, 88...108, 134...174, 370...512, 1100...1300 МГц.

Для передач используют сигналы с частотной широкополосной (WFM) и узкополосной (NFM) модуляцией несущей. Ширина спект-

ра излучаемого сигнала составляет при WFM 50...120 кГц, при NFM 6...12 кГц, что позволяет значительно увеличить дальность передачи при наличии специального приемника. Для повышения скрытности используют также сложные шумоподобные сигналы, передачи с псевдослучайной перестройкой несущей частоты и кодирование информации. Кроме того, в связи с бурным развитием беспроводной связи стали активно использоваться так называемые «легальные» закладки, использующие для передачи информации диапазон частот сотовой связи. К этому виду закладочных устройств можно отнести специально доработанные сотовые телефоны и закладочные устройства, разработанные с использованием элементов сотового телефона.

Рассмотрим основные группы изделий, предназначенных для непосредственного ручного поиска и обнаружения местоположения закладочных средств, передающих информацию по радиоканалу, классифицируя их по принципу построения и функциональным возможностям.

2.1. Индикаторы электромагнитных излучений

Принцип действия индикаторов поля (ИП) основан на широкополосном детектировании сигнала в контролируемом помещении. Наиболее распространенный диапазон 50...3000 МГц (самые совершенные образцы — до 8 ГГц). Дальность обнаружения от 0,3 до 3 м (зависит от электромагнитного фона в помещении и мощности передатчика СТС НСИ). Основной принцип обнаружения — амплитудный. Основные способы идентификации — индикатор уровня, частотомер (у наиболее совершенных моделей — идентификация известных цифровых сигналов). Дополнительные возможности: ведение электронного протокола «тревог». Возможные виды индикации: световая звуковая, ЖКИ, вибросигнал. Контроль производит лицо, осуществляющее режимное мероприятие.

Более детально остановимся на устройстве и принципе функционирования этих приборов.

Простейший индикатор состоит из слабонаправленной антенны линейной поляризации, широкополосного радиоусилителя, амплитудного детектора и порогового устройства. Такая конструкция прибора позволяет с его помощью обнаруживать работающие радиозакладки, использующие для передачи информации практически любые виды сигналов (рис. 2.1).

Поскольку в индикаторе поля отсутствуют входные цепи селекции сигналов, то он не способен сканировать частотный диапазон и реагирует на появление сигналов радиозаладочных устройств (ЗУ) практически мгновенно, независимо от частоты передачи. В последнее

Рис. 2.1. Структурная схема индикатора электромагнитных излучений

время на рынке появились селективные ИП, работающие по принципу сканирующего приёмника, но с более широкой полосой обзора.

За счет того, что полоса пропускания индикатора поля обычно равна несколько ГГц, чувствительность таких приборов составляет от 1 до 10 мВ, в связи с чем дальность обнаружения ЗУ невысока, на практике составляет единицы метров («ближняя зона») и сильно зависит от рабочей частоты и мощности ЗУ. В основном, это свойство индикаторов поля и определило порядок их применения при проведении поисковых мероприятий.

Прибор регистрирует интегральный уровень электромагнитных излучений в месте приема. В случае, когда текущее значение превысит установленный порог, соответствующий естественному уровню внешних излучений (фону), срабатывает световая или звуковая сигнализация.

Радиозакладка обнаруживается в том случае, когда интенсивность создаваемого ею электромагнитного поля превышает уровень фоновых излучений.

Введение в схему индикатора усилителя низкой частоты и громкоговорителя дает возможность выделить на фоне внешних сигналов тестовый акустический сигнал, т. е. реализовать акустическую завязку, суть которой состоит в следующем. Модулированное тестовым звуковым сигналом излучение принимается антенной индикатора, детектируется и после усиления поступает на вход динамика. В определенных условиях между микрофоном радиозакладки и динамиком индикатора может установиться положительная обратная связь, проявляющаяся в виде характерного звукового сигнала, напоминающего свист.

Индикаторы электромагнитных излучений характеризуют следующие параметры:

- рабочий диапазон частот;
- чувствительность по напряженности электромагнитного поля;
- радиус обнаружения закладки с известной мощностью радиопередатчика;
- пределы регулирования порога чувствительности, методы ее повышения;
- наличие режима акустической завязки;

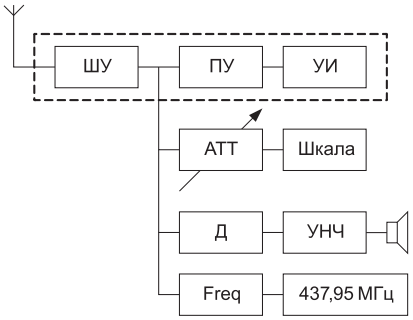


Рис. 2.2. Блок-схема профессионального индикатора поля: ШУ — широкополосный усилитель; ПУ — пороговое устройство; УИ — устройство индикации; АТТ — аттенюатор; Шкала — устройство индикации уровня; Д — демодулятор; УНЧ — усилитель нижних частот; Frec — частотомер

- тип индикации;
- возможность прослушивания информации, передаваемой радиозакладкой;
- тип источника электропитания и время непрерывной работы от него в режимах обнаружения и поиска;
- габариты, масса, конструкция.

В зависимости от решаемых с помощью индикаторов поля задач можно провести их классификацию и условно разделить на:

- бытовые индикаторы электромагнитного поля;
- профессиональные индикаторы электромагнитного поля.

Бытовые индикаторы электромагнитного поля. Как правило, единственной функцией бытовых индикаторов поля является включение индикации при превышении уровнем электромагнитного поля некоторого ранее установленного значения (порога). Индикация таких приборов, как правило, имеет смысл «Да/Нет». Индикаторы предназначены для информирования владельца о наличии (появлении) в ходе переговоров или в месте нахождения владельца ИП несанкционированных излучений, превышающих фоновое значение излучений в данном месте. Приборы имеют малые габариты, скрытую индикацию. В большинстве своем они закамуфлированы под часто используемые бытовые приборы и различного рода сувениры: брелоки для ключей, пульты включения автомобильной сигнализации, авторучки («Спутник», «Комар», Antibug+, «Блокнот», «Hunter ручка-детектор» и т. д.).

Профессиональные индикаторы поля имеют расширенные функциональные возможности. Как правило, в их состав включаются: частотомер, аттенюатор, устройства для осуществления акустической завязки и режекторные фильтры. Блок-схема профессионального индикатора поля представлена на рис. 2.2.

Так как эффективность индикаторов поля сильно зависит от помеховой обстановки в конкретном месте поиска, то для уменьшения

этой зависимости в некоторых моделях ИП используются режекторные или полосовые фильтры (АПП-7). Первые в значительной степени уменьшают уровень помех от известных источников (как правило, передатчиков телевещания) и настроены на наиболее мощные из них. Вторые сужают частотный диапазон поиска, чем уменьшают мощность помех на входе прибора. Обычно применяется несколько полосовых фильтров, каждый из которых настроен на свой диапазон частот. Вместе они перекрывают диапазон частот индикатора поля. При поиске в зависимости от загрузки проверяемого диапазона фильтры могут использоваться выборочно.

Режим акустической завязки и возможность определения частоты источника радиоизлучения в меньшей степени влияют на эффективность поиска и, в основном, предназначены для дополнительной идентификации источника радиосигнала с целью определения: опасный/неопасный.

Режим частотомера позволяет измерять значение несущей частоты радиосигнала, уровень которого значительно превышает уровень фона. Это дает возможность первично идентифицировать передатчик по значению несущей частоты. Режим частотомера полезен, когда известно значение несущей частоты ЗУ и стоит задача конечной локализации передатчика опасного сигнала. Например, при использовании автоматизированных комплексов радиоконтроля поиск и идентификация могут проводиться автоматически. При этом несущая частота ЗУ будет определена комплексом, а локализацию удобней осуществлять при помощи индикаторов поля, имеющих режим частотомера (RAKSA-101, RAKSA-120, «Блик-Д», «Оберег», ST-107, ST-110, «Флик»).

Мы уже говорили о том, что информация, выводимая на устройство индикации, имеет немаловажное значение при определении принадлежности обнаруженных излучений к работе ЗУ. Устройства индикации современных индикаторов поля можно разделить на два основных вида: светодиодные и цифровые, выводящие информацию об обнаруженных сигналах на дисплей прибора.

Принципиально светодиодная индикация (рис. 2.3) представляет собой дорожку светодиодов, загорающихся при обнаружении сигнала, превышающего уровень порогового значения электромагнитного поля. По количеству загоревшихся светодиодов оператор делает вывод о возможном местонахождении источника излучения (чем ближе источник излучения, тем больше амплитуда принимаемого сигнала и большее число светодиодов загорится).

Рассмотрим цифровые устройства индикации, выводящие информацию об обнаруженных сигналах на дисплей (рис. 2.4).

Рис. 2.3. Устройства индикации светодиодных индикаторов поля

Рис. 2.4. Образцы цифровых индикаторов поля

Устройства индикации современных цифровых индикаторов поля позволяют выводить на дисплей следующую информацию: частоту обнаруженного сигнала, мощность излучения в децибелах или по количеству закрашенных секторов, а также принадлежность к известным видам излучения (GSM, DECT, Bluetooth и Wi-Fi). Такой объем выводимой информации позволяет оператору определить в зависимости от частотной области излучения принадлежность сигнала к тому или иному виду и локализовать его источник. Кроме того, у некоторых цифровых индикаторов имеется возможность производить селекцию обнаруженных сигналов и в данный момент работать только с тем сигналом, который вас интересует. Многие из цифровых индикаторов имеют возможность подключения к персональному компьютеру, что также расширяет их возможности.

Таким образом, проведенный краткий анализ тактических возможностей поисковых индикаторов с различной индикацией информации об обнаруженных излучениях позволил сделать определенные выводы:

- светодиодная индикация не обеспечивает оператора необходимой

информацией для идентификации обнаруженного сигнала, даже для ЗУ с открытым каналом передачи данных;
- при наличии мощного внешнего излучения (например, от находящейся рядом с контролируемым помещением базовой станции сотовой связи) светодиодный индикатор будет реагировать только на этот сигнал, что не позволит выявлять излучение ЗУ из защищаемого помещения;
- информация, выводимая на дисплеи цифровых индикаторов поля, а именно частота, мощность излучаемого сигнала и принадлежность импульсных сигналов к определенному виду, позволяет оператору с более высокой вероятностью выявить принадлежность излучаемых сигналов к определённому источнику излучения;
- наличие системы селекции обнаруженных сигналов позволяет отстроиться от источника помехового сигнала и анализировать сигналы, подходящие по параметрам к излучениям ЗУ.

Единственным недостатком цифровых индикаторов поля по сравнению со светодиодными является их более высокая стоимость, но, как известно, скупой платит дважды.

Рис. 2.5. Анализатор электромагнитного поля «Кордон»

Анализируя рынок поисковых технических средств можно выделить ряд цифровых индикаторов, которые по своим параметрам и характеристикам удовлетворяют требованиям, предъявляемым к поисковым приборам. К ним можно отнести анализатор электромагнитного поля «Кордон», детекторы электромагнитного поля ST-107, ST-110, селективные индикаторы поля RAKSA-101, RAKSA-120, универсальный прибор РИЧ-8. Дадим краткую характеристику каждому из перечисленных приборов.

Анализатор электромагнитного поля «Кордон» (рис. 2.5) предназначен для выявления и локализации маломощных источников электромагнитного излучения в диапазоне от 50 до 8000 МГц. Анализатор поля позволяет выявлять закладочные устройства, внедренные в выделенные помещения и на объекты информатизации и использующие для передачи информации радиоканал. Работа анализатора основана на интегральном методе измерения уровня электромагнитного поля в точке его расположения. Прибор позволяет идентифицировать сигналы устройств сотовой и телефонных систем связи стандартов GSM-900, GSM-1800 (DCS), DECT, а также беспроводных систем связи Bluetooth и Wi-Fi (диапазон 2,4 ГГц) и позволяет не только обнаружить излучение радиопередатчика, негласно установленного в выде-

ленном помещении, но и измерить частоту его сигнала, а также оценить мощность электромагнитного излучения в точке приема. Прибор имеет два режима: режим поиска и режим акустической завязки. В режиме поиска осуществляется измерение частоты и уровня электромагнитного излучения. В режиме акустической завязки возможен поиск радиопередатчиков методом акустической обратной связи. Прибор снабжен жидкокристаллическим дисплеем, на котором отображаются: диапазон частот; уровень и частота принимаемого сигнала; наличие сигналов GSM-900, GSM-1800, DECT, Bluetooth, Wi-Fi; уровень порога обнаружения и заряда элементов питания.

Детектор электромагнитного поля ST-107 (рис. 2.6) предназначен для выявления и локализации маломощных источников электромагнитного излучения в диапазоне от 50 до 7000 МГц. Большой набор встроенных эффективных инструментов: частотомера, графического и цифрового индикаторов уровня принимаемого сигнала, осциллографа, самописца позволяет успешно выявлять и локализовать радиомикрофоны, телефонные радиоретрансляторы, радиостетоскопы, видеокамеры с радиоканалом, технические средства пространственного ВЧ навязывания, радиомаяки, сотовые телефоны и радиомодемы стандарта GSM, беспроводные телефоны стандарта DECT, устройства передачи информации с использованием стандартов Bluetooth, WLAN, а также возможность идентификации принимаемых цифровых сигналов (GSM, DECT, Bluetooth, WLAN). Информация выводится на графический цветной OLED-индикатор. Специальное программное обеспечение обеспечивает работу ST-107 под управлением персонального компьютера, что расширяет возможности по визуализации полученной информации, ее архивированию для последующего анализа.

Рис. 2.6. Детектор электромагнитного поля ST-107

Детектор поля ST-110 (рис. 2.7) предназначен для обнаружения и локализации радиоизлучающих специальных технических средств (РСТС) негласного получения информации: радиомикрофонов, телефонных радиоретрансляторов, радиостетоскопов, скрытых видеокамер с радиоканалом передачи информации, технических средств систем пространственного высокочастотного облучения в радиодиапазоне, технических средств передачи изображения с монитора ПЭВМ по радиоканалу, радиомаяков систем слежения за перемещением объектов (людей, транспортных средств, грузов и т. п.). Кроме того, несанкционированно включенные радиостанции, радиотелефоны и телефоны с радиоудлинителем, излучения используемых сотовых радио-

Рис. 2.7. Индикатор поля ST-110

телефонов стандарта GSM и DECT, несанкционированно используемых устройств с протоколом передачи данных Bluetooth и 802.11... (WLAN, Wi-Fi) в частотном диапазоне 2,4 ГГц.

Перечисленные выше поисковые приборы с расширенным частотным диапазоном могут успешно использоваться при выполнении поисковых работ при защите сведений, составляющих государственную тайну. Применение противником современных СТС для получения такой информации вызывает необходимость использования всех потенциальных возможностей этих приборов, что предъявляет повышенные требования к уровню подготовки поисковиков.

Защита от утечки информации, составляющей коммерческую тайну или относящейся к информации, в отношении которой владельцем установлено требование об обеспечении ее конфиденциальности, имеет свои особенности. Эти особенности прежде всего связаны с возможностями злоумышленников. Как правило, эти возможности ограничены незаконными предложениями радиорынков и различных «шпионских» сайтов в Интернете. Другой аспект данной проблемы связан с уровнем подготовки поисковиков. При защите сведений, составляющих коммерческую тайну, в условиях нашей действительности большинство коммерсантов стараются своими силами устранить возникшие проблемы и ставят задачу по выявлению ЗУ собственным работникам служб безопасности, а это, как правило, лица, имеющие недостаточную подготовку в данной области. Это налагает определенные требования к применяемым поисковым приборам. Они, при хороших технических характеристиках, должны иметь удобную схему управления, хороший интерфейс и достаточную и понятную информацию об обнаруженных сигналах, выводимую на устройство индикации. Такими параметрами обладает селективный индикатор поля RAKSA-120.

Рис. 2.8. Селективный индикатор поля RAKSA-120

Селективный индикатор поля RAKSA-120 (рис. 2.8) предназначен для обнаружения в ближней зоне и определения местоположения радиопередающих устройств, использующихся для негласного съема аудио- и видеоинформации.

По принципу действия селективный индикатор поля RAKSA-120 представляет собой скоростной супергетеродинный приемник с низкой ПЧ и синтезатором частоты. Время цикла сканирования и анализа всех циф-

ровых и аналоговых сигналов не превышает 1,5 с. Индикатор поля RAKSA-120 может работать в режимах охраны, обзора, поиска, поиска с вычитанием спектра и мониторинга цифровых сигналов. Особенности индикатора поля RAKSA-120: селективный прием радиосигналов, высокая скорость сканирования и анализа, обнаружение широкополосных и цифровых сигналов, адаптация к фону в режиме охраны, возможность поиска с вычитанием спектра, аудиоконтроль сигналов, измерение частоты и уровня сигнала, журнал событий тревоги, бесшумная индикация тревоги (вибросигнал), отсутствие внешней антенны. Наиболее оптимальным для ведения поиска активных ЗУ в сложной радиоэлектронной обстановке является режим обзора. В этом режиме индикатор производит широкополосное сканирование во всем диапазоне частот (от 50 до 3200 МГц). Обнаруженные в процессе сканирования излучения, превышающие заданное пороговое значения, выводятся в виде списка на дисплей с указанием частоты и уровня обнаруженного сигнала. В этом режиме оператор имеет возможность выделить интересующее его излучение и в дальнейшем работать только с этим сигналом до обнаружения источника излучения.

Индикатор поля SEL SP-222 (рис. 2.9). Цифровой индикатор поля предназначен для обнаружения и локализации любых работающих источников радиоизлучения в ближней зоне, а также сотовых телефонов стандартов GSM, DAMPS, MPS, DECT, беспроводных видеокамер, устройств Wi-Fi и Bluetooth. Может работать в следующих режимах: в режиме поиска; в режиме целенаправленного обнаружения цифровых сигналов GSM и DECT; в сторожевом режиме.

Рис. 2.9. Индикатор поля SEL SP-222

Кроме того, для более точной локализации источника излучения может использоваться режим акустозавязки.

Индикатор поля SEL SP-77/2M «Ловец» (рис. 2.10) предназначен для оперативного обнаружения и поиска радиоизлучающих устройств, имеющих минимальную мощность излучения. Он позволяет обнаружить электромагнитное излучение, оценить относительный уровень сигнала и найти его источник в диапазоне частот. Индикатор имеет следующие режимы работы:

Рис. 2.10. Индикатор поля «Ловец»

Режим поиска со звуковой, световой и виброиндикацией предназначен для обнаружения скрытно установленных радиопередающих устройств съёма информации. Световая индикация на 8-сег-

ментной светодиодной шкале позволяет оценить расстояние до закладки и упрощает её поиск. При необходимости звуковая и виброиндикация могут быть отключены.

Режим акустозавязки (обратной акустической связи). Используется для идентификации обнаруженного излучения, позволяя выделить излучение закладки на фоне других радиосигналов. Появившийся в динамике после включения этого режима характерный свист говорит о том, что в непосредственной близости находится работающее радиопередающее устройство с микрофоном.

Сторожевой режим. Позволяет при минимальном потреблении электроэнергии обнаруживать вновь появляющиеся в обследованном помещении неизвестные излучения.

Режим обнаружения импульсных сигналов. Предназначен для обнаружения импульсной цифровой передачи: мобильных телефонов стандартов GSM, DCS-1800, DECT (кроме CDMA).

Рис. 2.11. Портативный измеритель мощности РИЧ-8

Портативный измеритель мощности РИЧ-8 (MFP-8000) (рис. 2.11) относится к семейству универсальных приборов, в которых органично сочетаются свойства присущие сразу нескольким типам измерительных приборов — измерителю мощности, частотомеру, индикатору поля и анализатору сигнатуры. Диапазон рабочих частот: 0,1...8000 МГц. Вход 50 Ом (не более 1 Вт), разъем N-типа. Динамический диапазон измерений уровня мощности 90 дБм, (от -60 до $+30$ дБм). Точность измерения уровня мощности $\pm 0{,}5$ дБм. Максимальная измеряемая мощность (со встроенным аттенюатором) 1 Вт. Чувствительность: при измерении частоты не хуже 13 мВ (-25 дБм) в диапазоне 0,1...8000 МГц и не хуже 1,2 мВ (-45 дБм) в диапазоне 300...6000 МГц; при измерении мощности не хуже $0{,}5 \cdot 10^{-8}$ Вт. КСВН не более 1,5. Диапазон рабочих температур от 0 до $+50$ °С.

Универсальный прибор ST-31M «Пиранья» (рис. 2.12) от своих предшественников отличается введением в его структуру в качестве измерительного элемента селективного приемника, что существенно расширило его информационные возможности.

ST-031M позволяет обнаружить каналы передачи: радиомикрофонов, радиостетоскопов и телефонных ретрансляторов, в том числе импульсных и со сложными видами модуляции; устройств, передающих информацию по силовым и слаботочным проводным линиям в надзвуковом диапазоне частот; микрофонов, передающих информацию по задействованным и выделенным слаботочным линиям в рече-

вом диапазоне частот; передатчиков, транслирующих информацию в инфракрасном, ультразвуковом и ультрафиолетовом диапазонах.

Кроме того, при помощи ST-031M можно выявить и качественно оценить акустический и вибрационный каналы утечки информации естественного происхождения. В приборе предусмотрен режим идентификации стандартных цифровых каналов передачи данных (GSM, DECT, Bluetooth, Wi-Fi).

ST-031M позволяет исследовать принятые сигналы в режимах анализатора спектра и осциллографа.

Рис. 2.12. Универсальный прибор ST-31M «Пиранья»

Функционально ST-031M «Пиранья» состоит из трех каналов обнаружения, каждый из которых предназначен для поиска сигналов в определенном диапазоне частот. Комплект антенн, датчиков и переходников позволяет адаптировать каналы обнаружения для поиска различных подслушивающих устройств и каналов утечки информации естественного происхождения. Информация о принятых сигналах и режимах работы выводится на цветной графический дисплей. Управление прибором производится при помощи удобной 12-кнопочной клавиатуры. Интерфейс ST031M прост и интуитивно понятен. При его разработке учитывался многолетний опыт эксплуатации предыдущих моделей прибора. «Пиранья» имеет возможность стыковки с ПЭВМ, что позволяет существенно расширить возможности прибора по визуализации и архивации информации. Кроме того, прибор может применяться для обнаружения и качественной оценки информативных электромагнитных полей, создаваемых оргтехникой и средствами связи, для поиска скрытой электропроводки, потенциально пригодной для использования в составе ЗУ. Использование акустического микрофона и вибродатчика позволяет выявить и качественно оценить вибрационные и акустические каналы утечки информации, а также проконтролировать эффективность систем виброакустической защиты помещений.

Применение для анализа различных сигналов одних и тех же органов управления и выведение на дисплей аналогичных изображений различных видов сигналов позволяют даже неопытному оператору успешно работать с прибором.

ST-031M поставляется в двух видах комплектации: базовая и расширенная. В расширенную комплектацию входят дополнительные антенны, адаптеры и аксессуары, которые позволяют наиболее полно реализовать технические возможности прибора.

Многофункциональное поисковое устройство ST-131 «Пиранья II» (рис. 2.13) предназначенно для проведения мероприятий по об-

Рис. 2.13. Общий вид ST-131 «Пиранья II»

наружению и определению местоположения специальных технических средств негласного получения информации, (закладочных устройств) и выявления естественных и искусственно созданных каналов утечки информации.

ST-131 «Пиранья II» позволяет выявить и локализовать: радиомикрофоны, включая устройства с накоплением информации и с псевдослучайной перестройкой частоты; телефонные радиоретрансляторы; радиостетоскопы; беспроводные видеокамеры; несанкционированно используемые сотовые телефоны и модемы стандартов GSM, DECT, а также устройства с цифровыми каналами передачи данных стандартов WLAN и Bleutooth; ЗУ, имеющие в своем составе устройства пространственного высокочастотного облучения; радиомаяки для слежения за перемещением объектов; ЗУ, использующие для передачи информации силовые линии сети переменного тока, абонентские телефонные линии, линии систем пожарной и охранной сигнализации; ЗУ с передачей информации в инфракрасном диапазоне частот; ЗУ с передачей информации в ультразвуковом диапазоне частот.

Кроме того, на дисплей прибора выводится большой объем информации о текущем состоянии анализируемого диапазона частот, что, с одной стороны, позволяет детально проанализировать обстановку, а с другой — предъявляет повышенные требования к подготовке оператора. Появившаяся в приборе возможность выбора для анализа любой полосы обзора позволяет оператору детально проанализировать выбранный частотный диапазон.

Программное обеспечение ST-131 Analyzer-pro существенно расширят возможности изделия по анализу сигналов. Заложенные в программное обеспечение возможности позволяют проанализировать большинство типов ЗУ, использующих различные виды закрытия передаваемой информации (рис. 2.14).

Работа прибора под управлением компьютера позволяет наиболее полно реализовать возможности по обнаружению различного ро-

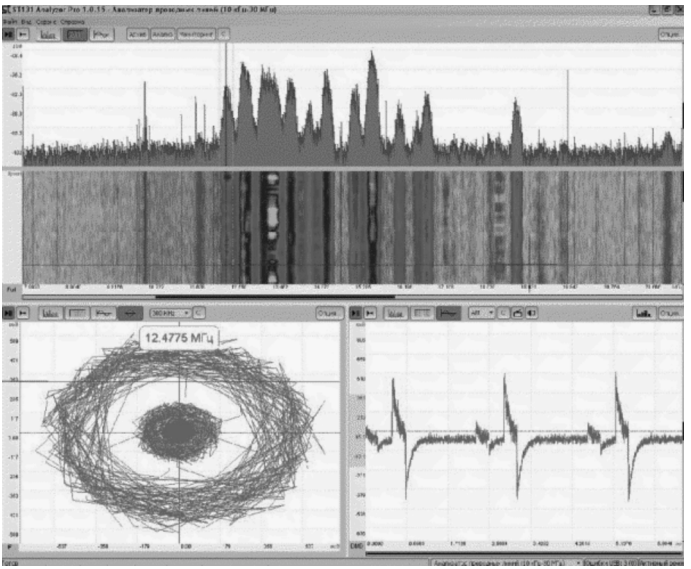


Рис. 2.14. Общий вид основного окна программы

Рис. 2.15. Вид «водопада» с сигналом ППРЧ

да ЗУ с различного рода закрытием канала передачи, а также сигналов, использующих для скрытия передачи различные виды дельта-модуляции, ППРЧ и другие виды закрытия.

Так, например, псевдотрехмерная плоскость («водопад») позволяет отследить характер передаваемых сигналов. Данный вид отображения помогает обнаружить и идентифицировать сигналы, излучение которых различно по частоте и времени (псевдослучайной перестройкой рабочей частоты, ППРЧ). На рис. 2.15 показан сигнал установления подключения стандарта Bluetooth, который можно отнести к сигналам с ППРЧ (ширина канала 1 МГц, длительность 0,625 мс).

Векторная диаграмма (рис. 2.16) является представлением сигнала в полярных координатах на комплексной плоскости. Полученный модуль вектора (на диаграмме показывается его конечная точка) отражает мгновенную амплитуду сигнала, а угол — текущее значение

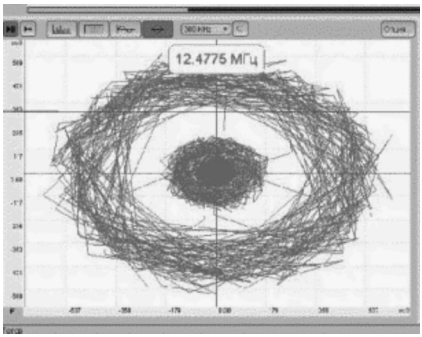


Рис. 2.16. Общий вид отображения векторной диаграммы

Рис. 2.17. Индикатор поля DP-20

фазы. Анализ траектории движения вектора позволяет идентифицировать амплитудно-модулированные, фазомодулированные, сигналы многопозиционной фазовой и смешанной амплитудно-фазовой модуляции.

К таким видам относятся, например, сигналы с такой модуляцией, как AM, PSK, QAM. Сигналы с постоянной амплитудой, например FM, будут выглядеть в виде окружности с центром в начале координат.

Таким образом, использование программной оболочки позволяет выявить при анализе большинство из существующих в настоящее время радиосигналов, но в то же время предъявляет повышенные требования к подготовке оператора. Так как такого рода система является автоматизированной, а не автоматической, то главную роль в ней играет оператор, и от уровня его подготовки, в полной мере, зависят грамотное использование прибора и результаты поиска.

Индикатор поля DP-20 (рис. 2.17) представляет собой электронный прибор, предназначенный для световой и звуковой индикации наличия и относительного уровня электромагнитного излучения в диапазоне частот от 900 МГц до 31 ГГц. Максимальная чувствительность 0,02 мкВт/см^2. Динамический диапазон индикатора 20 дБ.

Индикатор позволяет обнаружить электромагнитное поле, оценить уровень сигнала и найти его источник. Возможность выбора режима акустической обратной связи или режима звуковой индикации уровня сигнала облегчает поиск радиопередающих устройств. Наличие регулировки усиления позволяет работать с детектором в условиях сложной электромагнитной обстановки и обеспечивает возможность точной локализации радиопередающих устройств. Антенна прибора имеет ярко выраженную диаграмму направленности, максимум которой совпадает с осью антенны. Это позволяет легко определять направление на источник излучения и обнаруживать его. Для прос-

лушивания акустических сигналов к прибору могут быть подключены головные телефоны, при этом встроенный динамик автоматически отключается. Десятисегментная логарифмическая светодиодная шкала и прерывистый тональный звуковой сигнал обеспечивают наглядность и удобство при работе с прибором, тональность звукового сигнала меняется в зависимости от уровня входного сигнала.

Перечисленные приборы реализуют оптимальные значения чувствительности при применении соответствующих антенн.

Применение цифровых технологий, использование ЖК дисплеев, новые функциональные возможности, присущие радиочастотомерам, значительно расширили область и эффективность применения индикаторов электромагнитных излучений. Однако при этом сохранился их существенный недостаток — обнаружение источника излучения только в непосредственной близости от него и, как следствие, иногда приходиться использовать радиочастотомеры.

2.2. Радиочастотомеры

В отличие от индикаторов поля радиочастотомеры регистрируют и частоту сигналов, превысивших установленный порог. Внешний вид радиочастотомеров приведен на рис. 2.18.

Изделие РИЧ-3 измеряет частоту сигналов, превысивших один из четырех задаваемых уровней (+ 3, + 6, + 12, + 18 и + 24 дБ) напряженности электромагнитного поля в диапазоне 100. . . 3000 МГц.

При обнаружении источника излучения на индикаторе, способном регистрировать сигналы с динамическим диапазоном 60 дБ, высвечивается частота принимаемого ВЧ сигнала, звучит тональный сигнал,

а) *б)* *в)* *г)*

Рис. 2.18. Внешний вид радиочастотомеров: *а* — РИЧ-3; *б* — ST-007; *в* — CUB; *г* — SCOUT

происходит засветка сегментов светодиодного устройства отображения. Чувствительность прибора при измерении частоты с точностью ±0,002 % не ниже 4,6 мВ на краях диапазона (100 МГц, 3000 МГц) и не ниже 1,5 мВ в диапазоне 300...2000 МГц. Выявление места установки радиозакладки производится методом акустической завязки или прослушиванием помещения через головные телефоны, фиксирующие реакцию на ритм, т. е. на постукивание вблизи подозрительных мест. В приборе введена возможность автоматической установки захваченной частоты (через порт RS-232) на сканирующих приемниках типа AR-3000, AR-8000 и др. Также имеется возможность измерения частоты передатчиков, работающих в стандарте GSM. Ток потребления от встроенного аккумулятора напряжением 7...9 В равен 100 мА при измерениях частоты и 300 мА в режиме акустозавязки. Габариты (без антенны) 155×55×38 мм.

Поисковое устройство ИПФ-6 функционирует в режиме широкополосного приема в диапазоне 30...500 МГц и в режиме узкополосного приема в поддиапазонах 30...60, 60...120, 120...250, 250...500 и 500...1500 МГц, имеет режекторные фильтры на частоты 49, 77, 172, 191, 215 МГц, которые позволяют реализовать в зоне действия мощных вещательных станций характеристики обнаружения аналогичные РТ-022. Встроенный частотомер измеряет частоту сигнала с точностью ±2 кГц.

В основу работы современных радиочастотомеров положен принцип мгновенного «захвата» частоты радиосигнала с последующей обработкой микропроцессорным блоком, производящим запись сигнала в устройство памяти, цифровую фильтрацию, проверку его на стабильность и когерентность. Значение частоты, измеряемой с точностью до единиц герц, отображается на индикаторе. В ряде приборов имеется возможность определения относительного уровня сигнала.

Портативный прибор М1 диапазона 10 Гц...2800 МГц может измерять частоты как радиосигналов, так и сигналов в элементах электрических схем при контактном подключении. М1 имеет цифровой фильтр, позволяющий исключить случайные результаты измерений, функцию автозахвата, память для сохранения трех последних результатов, высокоомный (для подключения щупов при контактных измерениях) и низкоомный (антенный) входы, а также внутренний асинхронный последовательный интерфейс с уровнями TTL. В случае подключения частотомера к компьютеру появляется возможность одновременного контроля частоты на дисплее и автоматического накапливания результатов в компьютерном файле как в режиме цифрового автозахвата, так и в режиме непрерывного измерения. Сформированные в файле данные имеют привязку к компьютерному времени и дате.

Благодаря высокой чувствительности усилителей прибор может применяться для обнаружения источников мощностью 1 мВт. Шестнадцатисегментный индикатор уровня сигнала позволяет достаточно точно локализовать радиомикрофоны и телефонные микропередатчики.

Портативный частотомер CUB диапазона 1...2800 МГц имеет цифровой фильтр и функцию автозахвата сигнала. Предварительная цифровая фильтрация дает возможность игнорировать случайные нестабильные сигналы, а функция автозахвата позволяет фиксировать на индикаторе измеренное значение частоты до выключения прибора.

CUB обладает возможностью отсчета частоты с пятью скоростями в диапазоне до 250 МГц и с тремя скоростями в диапазоне до 2800 МГц. При минимальном времени счета 1 с, точность измерения частоты в диапазоне до 250 МГц составляет 1 Гц.

Высокая чувствительность прибора позволяет регистрировать источники радиоизлучения мощностью от 2 до 5 мВт на удалении в несколько метров.

Прибор SCOUT работает в частотном диапазоне 10...1400 МГц. Кроме основных режимов, свойственных частотомерам M1 и CUB, SCOUT способен обнаруживать, регистрировать и запоминать 400 значений частот, а также фиксировать до 255 случаев активности источников излучения на каждой из этих частот с чувствительностью не хуже 5 мВ в диапазоне 30...900 МГц. Факт обнаружения новой частоты или повторной регистрации частоты, значение которой занесено в память, прибор сопровождает коротким звуковым или вибрационным сигналом (в случае новой частоты — одиночным, в случае уже записанной в память — двойным).

SCOUT имеет интерфейсы двух типов, позволяющие автоматически, практически мгновенно, перестраивать подключаемые к нему сканирующие приемники на зафиксированную частоту:

- полудуплексный, последовательный, стандарта CI-V, для управления приемниками IC-R10, IC-R8500, IC-R9000;
- дуплексный, для управления приемниками AR-8000, AR-8200.

Используя этот же порт, прибор можно подключить к IBM-совместимому компьютеру через универсальный интерфейс OPTOLINX.

Благодаря предварительной фильтрации и проверке сигнала на когерентность SCOUT фиксирует на 10-разрядном жидкокристаллическом дисплее только частоты источников радиоизлучения, игнорируя побочные сигналы от радиоэлектронной аппаратуры, работающей в ближней зоне. Объединение со сканирующим приемником дает возможность не только определить источник излучения, но и прослушать характерное звучание контролируемого канала.

Шестнадцатисегментный индикатор позволяет оценивать относительный уровень сигналов с точностью 3 дБ на 1 сегмент.

Портативный многофункциональный частотомер 3000A+ диапазона 10 Гц... 3000 МГц позволяет измерять как периодические, так и импульсные сигналы напряжением до 50 В, при минимальной длительности одиночного импульса 200 нс. Цифровой фильтр на базе микропроцессора позволяет игнорировать некогерентные фоновые излучения, исключая ложные срабатывания в режиме автозахвата. Внутренняя память хранит три последних результата измерений.

Наличие четырех входных усилителей, выведенных на два BNC-входа, и разбивка рабочего диапазона на 3 участка позволяют реализовать максимальную для таких приборов чувствительность.

Частотомер 3000A+ имеет внутренний интерфейс RS-232 для подключения к IBM-совместимому компьютеру.

Устройства отображения информации на панели управления прибора идентичны индикатору и дисплею частотомера SCOUT. Питание — аккумуляторы или адаптер 12 В (250 мА). Габариты металлического корпуса 135×100×35 мм.

Перечисленные радиочастотомеры реализуют оптимальные значения чувствительности при применении соответствующих антенн:

Антенна	Диапазон частот, МГц
TA100S	100... 500
RD27	< 50
RD100	100... 250
RD440	150... 500
RD800	> 500
DB32	150... 1300

Пример сравнения средней чувствительности радиочастотомеров РИЧ-3 и SCOUT-40 приведен на рис. 2.19.

В настоящее время в связи с появлением современных цифровых индикаторов поля потребность в использовании частотомеров снизи-

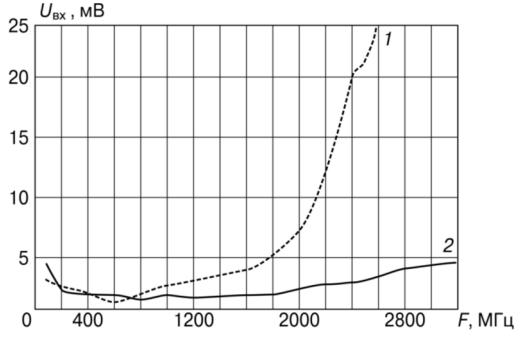


Рис. 2.19. Средняя чувствительность радиочастотомеров:
1 — РИЧ-3; *2* — SCOUT-40

лась. Кроме того, необходимо учитывать и наличие существенного недостатка индикаторов поля и частотомеров — их недостаточную чувствительность. Таким образом, с их помощью можно обнаружить источник излучения только в непосредственной близости от него, что вызывают необходимость использования более мощных и чувствительных приборов, а именно скоростных приемников ближней зоны.

2.3. Радиоприемные устройства

Скоростные приемники ближней зоны по сути своей являются сканирующими радиоприемниками. Поиск сигналов производится последовательным проходом всего диапазона с узкой полосой обзора. Скорость обзора диапазона (с учетом обработки сигналов) составляет несколько минут. Используются либо в контролируемом помещении, либо в помещении, смежном с контролируемым. Наиболее распространенный диапазон 50...3000 МГц. Дальность обнаружения до 10...15 м в зависимости от мощности передатчика специальных технических средств (СТС) несанкционированного съема информации (НСИ). Основной принцип идентификации «опасных» сигналов — анализ информации, заложенной в демодулированный сигнал (как частный случай — корреляционная обработка). Дополнительные возможности — создание списка «легальных сигналов». Способы индикации — световая, звуковая, индикатор уровня, частотомер, возможность прослушивания демодулированного сигнала.

Уникальными возможностями для обнаружения обладают высокоскоростные приемники. Они способны автоматически в течение долей секунды, просмотреть диапазон от единиц до нескольких тысяч мегагерц, зафиксировать частоту сигнала, уровень которого превышает интенсивность радиофона на 15...20 дБ, и обеспечить в реальном времени прослушивание информации, передаваемой по радиоканалам с АМ и ЧМ.

По массогабаритным показателям и функциональным возможностям сканирующие приемники можно условно разделить на переносимые и перевозимые. Хотя в настоящее время в связи с резкой миниатюризацией электронных компонентов такое разделение крайне условно. К переносимым приемникам относятся малогабаритные аппараты массой, как правило, не более 350 г, имеющие автономные источники питания. Эти приборы в диапазоне частот 100 (500) Гц... 2600 (3000) МГц осуществляют прием сигналов с амплитудной (AM), узкополосной (NFM) или широкополосной (WFM) частотной модуляцией. Некоторые образцы приемников регистрируют сигналы однополосной AM (SSB), передаваемые на частотах верхней боковой полосы (USB) или нижней боковой полосы (LSB), а также радиотелеграфные посылки (CW). При приеме с отношением сигнал/шум 10 дБ/мкВ

чувствительность сканеров 0,35...1 мкВ для NFM и 1...6 мкВ для WFM. При шаге перестройки от 50...500 Гц до 50...1000 кГц скорость сканирования достигает 20...30 каналов в секунду и более.

Сведения о частоте сигналов фиксируются в устройствах памяти емкостью от 100 до 4000 независимых каналов. Большинство аппаратов могут работать под управлением ПЭВМ.

Перевозимые приемники, отличающиеся габаритами и массой, достигающей до 20 кг, обладают значительно большими возможностями, почти все образцы управляются от ПЭВМ.

Широкое внедрение компьютерных технологий вызвало появление нового поколения сканеров.

Рис. 2.20. Сканирующий приемник ICOM IC-R20

Сканирующий приемник ICOM IC-R20 (рис. 2.20) предназначен для измерения параметров приемопередающих радиотехнических устройств. Приемник имеет возможность: осуществления двойного приема, т. е. контроль одновременно двух частот; прием одновременно радио- и ТВ сигнала; работает на частотах от 150 кГц до 3304,999 МГц в режимах SSB, CW, AM, FM, WFM с шагом перестройки от 0,01 до 100 кГц; имеет встроенный цифровой диктофон с объемом памяти 32MB; прием сигналов с кодовым и тональным разделением каналов; по субтонам возможно сканирование 1000 стандартных каналов памяти, 200 автоматически сканируемых каналов и 25 пар границ сканирования; до 11 часов непрерывной работы. IC-R20 может работать от трех пальчиковых батареек AA. Длительная работа, также как и зарядка встроенного аккумулятора, возможна от прикуривателя автомобиля или входящего в комплект адаптера.

Иногда прослушивания сигнала недостаточно, поэтому IC-R20 имеет спектроскоп. Он используется для отображения сигнала, на частоту которого настроен приемник. Спектроскоп работает независимо от прослушивания сигнала.

Скорость сканирования — до 100 каналов в секунду в режиме VFO. VSC (Voice Squelch Control) открывает шумоподавитель только при обнаружении модулированного сигнала.

Кроме того, возможно использование программируемого разноса частот (Offset monitor) для прослушивания полудуплексных каналов; автоматическое шумоподавление с функцией монитора; встроенного аттенюатора и контроля RF усиления; подавителя импульсных помех (noise blanker), автоматического ограничителя шума (Auto Noise Limiter), AF фильтра; AFC (Auto Frequency Control) функции АПЧ;

интерфейса CI-V для удаленного управления с PC (возможно при помощи дополнительного блока CT-17).

Приемник имеет: встроенную ферритовую антенну для AM сигнала; возможность использовать провода наушников как FM антенну; функцию ускоренного набора; функцию блокирования кнопок; функции автоматического отключения и сохранения энергии; стандартные ТВ и коротковолновые каналы в памяти.

Портативный прибор «Скорпион» (рис. 2.21) в автоматическом режиме позволяет за 15 с просмотреть диапазон 30...2000 МГц. После обнаружения нелегального передатчика с узкополосной или широкополосной ЧМ прослушать сигнал или подавить канал его приема, поставив на установленной частоте прицельную шумовую помеху, создаваемую встроенными генератором шума и модулятором. Управляющая микроЭВМ дает возможность запомнить значения 524 частот, 128 из которых могут быть затем исключены при повторном анализе радиообстановки. При полосе пропускания на промежуточной частоте 200 кГц чувствительность приемника в поддиапазоне 30...1000 МГц не превышает 50 мкВ, а в поддиапазоне 1...2 ГГц — 1000 мкВ. На жидкокристаллическом 16-разрядном индикаторе отображается информация о частоте и уровне входного сигнала. Габариты корпуса (без антенн) — 165×90×29 мм.

Рис. 2.21. Портативный прибор «Скорпион 3.5»

Скоростной поисковый приемник «Скорпион-XL» (рис. 2.22) представляет собой новую разработку в серии поисковых приемников «Скорпион». От предыдущих серий его отличает расширенный до 2500 МГц диапазон, удобный графический дисплей, позволяющий выводить спектрограмму исследуемого диапазона, а также компьютерный интерфейс. «Скорпион-XL» сохранил все основные черты своих предшественников. Это портативное средство радиотехнического контроля, предназначенное для автоматического обнаружения сигналов, излучаемых нелегальными радиопередатчиками, и подавления каналов их приема.

Рис. 2.22. Прибор «Скорпион-XL»

«Скорпион-XL»позволяет: изучать радиоэлектронную обстановку в режиме панорамного обзора диапазона 120...2500 МГц с полосой 20 МГц с последующим просмотром выбранного канала с полосой 200 кГц и спектрограммой с разрешением 5 кГц; обнаруживать

и определять местоположение нелегально существующего передатчика с использованием разнесенного приема на две антенны и контроля уровня гармоник; подавлять канал приема сигнала обнаруженного нелегального передатчика с помощью постановки на его частоте прицельной помехи; обнаруживать работающие телефоны сотовой связи стандарта GSM с индикацией диапазона частот, радиотелефоны стандарта DECT; осуществлять поиск в одном–трех программируемых участках диапазона частот; просматривать и редактировать три буфера памяти обнаруженных сигналов и исключенных каналов приема; проверять работоспособность приемников, индикаторов поля, частотомеров и других технических средств при помощи встроенного тестового генератора.

Диапазон принимаемых частот 30...2500 МГц. Чувствительность: в диапазоне 30...1000 МГц не хуже 30 мкВ, в диапазоне 1000...2500 МГц не хуже 100 мкВ. Выходная мощность тестового генератора/генератора помехи: в диапазоне 40...1000 МГц не менее 50 мкВ, в диапазоне 1000...2500 мГц не менее 10 мкВ. Режимы сканирования (шаг 200 кГц, подстройка 10 кГц): автонастройка, автозапись, автоисключение, поиск. Время сканирования диапазона не более 15 с. Поиск и индикация сигналов в диапазонах GSM, DECT, Bluetooth.

Рис. 2.23. Скоростной поисковый приёмник-коррелятор SEL SP-81 «Оракул»

Скоростной поисковый приёмник-коррелятор SEL SP-81 «Оракул» (рис. 2.23) предназначен для оперативного обнаружения работающих устройств съема акустической информации, использующих радиоканал. Наличие пассивного акустического коррелятора позволяет бесшумно и скрытно выявлять источники радиоизлучения, модулированные аналоговыми сигналами (радиомикрофоны) в автоматическом режиме без участия оператора. В приемнике предусмотрены два режима работы: поисковый — для обнаружения и локализации источников радиоизлучений и сторожевой — для непрерывного контроля за радиообстановкой в реальном времени. При обнаружении сигнала индицируются его частота и уровень, а демодулированный сигнал может воспроизводиться через встроенный громкоговоритель. Приемник обнаруживает радиопередатчики с мощностью в антенне 5 мВт на расстоянии не менее 5 м. Время сканирования всего частотного диапазона зависит от помеховой обстановки и составляет в среднем несколько секунд. Используемый в приборе метод корреляции предназначен для выявления радиомикрофонов и основан на сравнении демодулированного радиосигнала с опорным акустическим, присутствующим в помещении. Для реализации этого алгоритма применён

Рис. 2.24. Мониторинговый приемник RS GigaJet

речевой сигнал, обладающий достаточным пик-фактором (т. е. изменением текущей мощности). Кроме того, этот метод позволяет обнаруживать радиопередатчики с закрытым аналоговым каналом, например с инверсией спектра.

Мониторинговый приемник RS GigaJet (рис. 2.24). Радиоприемное устройство предназначено для решения задач радиомониторинга, обнаружения несанкционированных передатчиков, в том числе использующих короткие сигналы с большой скважностью, задач измерения параметров радиосигналов, получения спектральных оценок в диапазоне частот от 20 МГц до 12 ГГц. Коэффициент шума не более 10 дБ. Входной импеданс 50 Ом. Избирательность по зеркальному каналу: до 2 ГГц не менее 80 дБ; свыше 2 ГГц не менее 45 дБ. Время установки частоты синтезатора при перестройке на 20 МГц не более 500 мкс. Спектральная плотность шумов первого гетеродина, приведенная к ВЧ входу, при отстройке на 10кГц не более 135 дБ/Гц. Долговременная нестабильность гетеродинов не хуже 10^{-8}. Минимальный шаг перестройки 1 Гц. Максимальный уровень входного ВЧ сигнала не более 10 дБм. Ширина просматриваемой в реальном времени панорамы 20 МГц. Разрешение в режиме панорамыдо 1 кГц. Мощность на выходе линейного приемника при компрессии 1 дБ составляет 20 дБм. Точка пересечения интермодуляции третьего порядка по выходу OIP3 32 дБ. Уровень комбинационных частот при закрытом входном тракте (R = 50 Ом) на входе не более −120 дБм.

Панорамное радиоприемное устройство содержит линейный приемник, или тюнер, цифровой вычислитель, преобразующий сигналы в цифровую форму и производящий основные математические опе-

рации для обнаружения, накопления, фильтрации и демодуляции сигналов, а также встроенный коммуникационный компьютер, осуществляющий общее управление приемником, ввод данных, визуальное отображение настроек и результатов текущего мониторинга и их передачу по стандартным интерфейсам, например USB-2,0 или LAN, конечному пользователю.

Шаг перестройки линейного приемника 1 МГц. Высокую стабильность приемника по частоте обеспечивает термостатированный опорный кварцевый генератор, обеспечивающий долговременную нестабильность частоты настройки приемника не хуже $\pm 10^{-7}$/год. Линейный приемник построен по схеме двойного (для частот выше 2 ГГц тройного) супергетеродина и имеет выход промежуточной частоты 140 МГц с полосой пропускания 20 МГц. После выхода ПЧ дальнейшая обработка сигналов осуществляется сразу в цифровом виде. Блок цифровой обработки сигналов (ЦОС) построен на базе цифрового вычислителя, основу которого составляют DSP фирмы Texas Instruments типа TMS320C6416 с фиксированной запятой и прямой цифровой конвертер DDC типа TI/GraychipGC 4016.

На входе блока использованы два АЦП со скоростью выборки 105 мегациклов в секунду и с разрядностью 14 битов. В полосе 20 МГц цифровая фильтрация и демодуляция сигналов могут осуществляться одновременно по 4 каналам. Цифровой приемник позволяет настраиваться на сигнал с точностью до 1 Гц. Загрузка специализированного программного обеспечения вычислителя осуществляется платой коммуникационного компьютера по шине USB 2,0. Приемник работает полностью в автономном режиме, выполняя установленные задания, либо управляется по компьютерной сети через встроенный контроллер LAN.

Встроенное программное обеспечение RS Digital Jet позволяет регистрировать любые новые, в том числе кратковременные, сигналы на фоне ранее подготовленной усредненной панорамы. Мониторинговый приемник GigaJet может быть спроектирован для распределенной системы мониторинга в двухканальной либо многоканальной конфигурации. В удаленных точках объекта размещаются линейные приемники с непосредственно подсоединенными антеннами. Сигналы с выходов промежуточной частоты 140 МГц транслируются магистральными усилителями по кабелю в центр, где осуществляется цифровая обработка сигналов, их регистрация и анализ. Предложенная схема позволяет контролировать радиодиапазон до 12 ГГц и выше в любых точках объекта. Необходимо отметить, что приемник является портативным устройством и не требует подключения внешнего компьютера для решения задач мониторинга, поиска несанкционированных передач и т. д.

Рис. 2.25. Скоростной поисковый приёмник AOR SR 2200

Сканирующий приемник AR-5000A в основном использовался в качестве приемника радиосигналов при создании автоматизированных программно-аппаратных комплексов ближней радиоразведки. По своим техническим характеристикам он обеспечивал достаточную скорость сканирования частотного диапазона при высокой чувствительности.

В июне 2008 года он был снят с производства. На замену ему фирма AOR выпустила ряд сканирующих приемников, специально предназначенных для создания программно-аппаратных комплексов радиоконтроля под компьютерным управлением.

AOR SR 2200 (рис. 2.25)— компактный широкополосный управляемый с ПК сканирующий приемник (black box receiver), работающий в диапазоне от 25 МГц до 3 ГГц и предназначенный для профессионального применения. Основная версия приемника не имеет традиционной передней панели, связь с ПК осуществляется с помощью интерфейсного кабеля (присутствуют оба порта — RS 232 или USB) — соответствующие разъемы выведены на заднюю панель. При необходимости передняя панель может поставляться отдельно. Приемник имеет высокую чувствительность и широкий динамический диапазон; управление с помощью ПК предоставляет широкие возможности и обладает большей функциональной гибкостью; наличие ПК предоставляет возможность обработки принимаемых радиосигналов с помощью специального программного обеспечения; в комплект входит программное обеспечение под Windows и полный перечень команд управления; малые габариты (200×31×230 мм) и вес (1,3 кг).

Профессиональный сканирующий приемник AR-ONE (рис. 2.26) в свое время явился серьезным шагом в развитии технологии приема.

Рис. 2.26. Профессиональный сканирующий приемник AR-ONE

AR-ONE пользовался большим спросом среди профессионалов. Он имеет широкий диапазон: 0,01...3300 МГц с сохранением высокой чувствительности; малые габариты и вес (157×58×270 мм, 2,2 кг), возможность мобильного использования. Обладает сверхвысокой стабильностью частоты. Температурная нестабильность равна $\pm 10^{-7}$ в температурном диапазоне $-10 \ldots 50$ °C (в моделях AR5000 и AR7030 $\pm 1{,}5 \cdot 10^{-6}$). Имеет следующие шаги перестройки: стандартный — 1, 10, 50, 100, 500 Гц, 1, 1,5; 6,25; 9, 10, 12,5; 20, 25, 30, 50, 100, 500 кГц; нестандартный — до 1 МГц с шагом 1 Гц. В приемнике 10 генераторов VFO; динамический диапазон не менее 90 дБ; избирательность по побочным каналам приема не менее 60 дБ; избирательность по соседним каналам приема не менее 55 дБ во всех режимах; уровень побочных излучений не более -57 дБ; возможность управления 99-ю AR-ONE от одного компьютера. При настройке предусмотрено несколько методов ввода частоты: с цифровой клавиатуры, специальными кнопками или с помощью ручки настройки. Приемник может использовать следующие виды модуляции: SSB (USB, LSB), CW, AM, FM, WFM, включая специальные виды: широкая и узкая AM (WAM, NAM), узкая FM (SFM). Предусмотрен режим автоматической установки вида модуляции и шага перестройки частоты по рабочему диапазону. Обеспечивается полное восстановление несущей в режиме SSB, улучшающее качество приема; тройное преобразование частоты; 1000 ячеек памяти; частота внешнего опорного генератора 10 МГц; аудиовыход 1,5 Вт при КНИ $<$ 10 %.

Для удобства и более эффективного использования в качестве ядра в программно-аппаратных комплексах на базе приемника AR-ONE разработан приемник AOR AR-ONE-C, являющийся новой версией профессионального приемника и предназначенный для применения в радиокомплексах для пеленгации, состоящих из нескольких взаимосвязанных приемников при обеспечении фазовой когерентности.

Профессиональный сканирующий приемник AR-ONE-C (рис. 2.27) предназначен для применения в радиокомплексах, состоящих из нескольких взаимосвязанных приемников при обеспечении фазовой когерентности.

В AR-ONE-C для достижения наилучшего фазового синхронизма применен метод разделения частот гетеродина. В дополнение к эта-

Рис. 2.27. Профессиональный сканирующий приемник AR-ONE-C

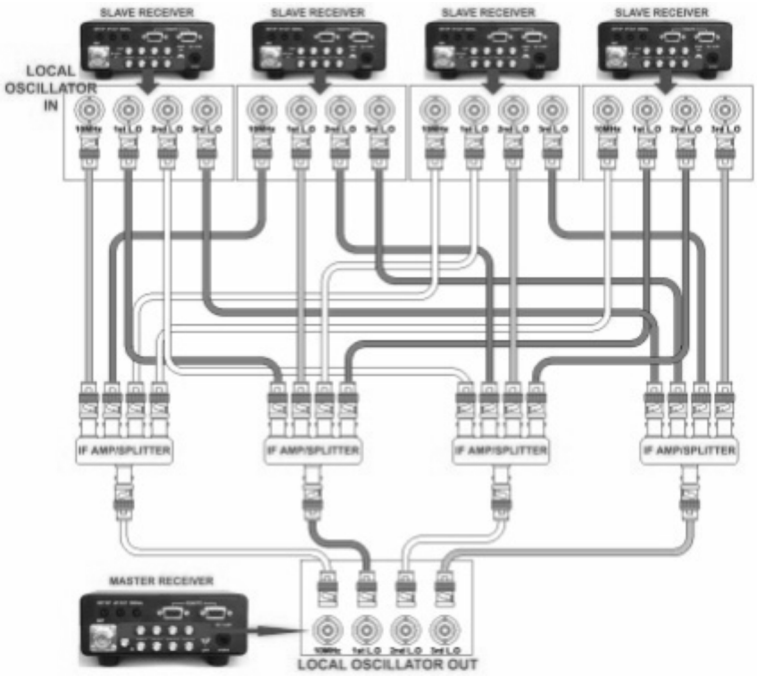


Рис. 2.28. Вариант объединения приемников

лонной частоте 10 МГц используются частоты 254,5 или 744,5 МГц и 10,245 МГц. При этом относительный фазовый сдвиг не превышает 5 %. Количество объединяемых в комплекс приемников ограничивается только характеристиками применяемых усилителей ПЧ и распределителей сигналов (рис. 2.28).

Мониторинговый приемник GigaJet (рис. 2.29), представляющий собой недорогую эффективную платформу для построения мощных многоканальных и многофункциональных систем радиоконтроля и радиоразведки. Объединенный с встроенным компьютером либо совместно с подключенным ноутбуком, приемник может быть как полностью автономной системой в стационарном или мобильном варианте, так и являться элементом или ячейкой, встроенной в большую территориально разнесенную систему, решающую поставленные задачи.

Приемник GigaJet содержит основной тюнер с преселектором и плату цифрового радио, конструктивно объединенные в блок, готовый к установке в 19-дюймовый корпус или мобильный кожух. Данная концепция даёт возможность быстро и гибко изменить конструктивное решение под требуемую системы.

Специализированное программное обеспечение позволяет исполь-

Рис. 2.29. Мониторинговый приемник GigaJet

зовать в проектируемой системе определенные компоненты для решения задач радиомониторинга различного уровня. Встроенные программные инструменты позволяют проводить скоростной спектральный анализ контролируемых диапазонов, распознавание вновь обнаруженных сигналов и их демодуляцию, а также прямую запись цифрового I/Q потока. Приемник GigaJet оптимизирован для удаленного управления по протоколу TCP/IP. Благодаря высокой скорости сканирования (5 ГГц в секунду) он способен обнаруживать кратковременные радиосигналы и сигналы с ППРЧ (FH). Приемник способен производить непрерывное (в реальном времени) накопление спектра сигнала в полосе до 2 МГц, что позволяет быстро обнаруживать широкополосные шумоподобные сигналы (DSSS — Direct Sequency Spread Spectrum), а также дает возможность быстрого накопления реализаций для создания фоновой панорамы. С помощью приемника можно за короткое время эффективно обследовать электромагнитную обстановку в открытом пространстве, здании, помещении и т. д. Кроме того, радиоприемное устройство способно решать задачи измерения параметров радиосигналов, получения спектральных оценок, демодуляции сигналов и т. д.

2.3.1. Режимы работы сканирующих приемников

Классифицируют три основных режима работы сканеров:

I — автоматическое сканирование в диапазоне частот;

II — автоматическое сканирование на фиксированных частотах;

III — ручное сканирование.

При реализации первого режима устанавливают границы диапазона сканирования, шаг перестройки частоты и вид модуляции. Для

сокращения времени возможно сканирование с пропуском частот, данные о которых занесены в память аппарата. Как правило, в современных сканерах имеется от 4 до 20 программируемых частотных диапазонов.

Существует несколько алгоритмов сканирования:

- сканирование прерывается, если уровень принимаемого сигнала превышает заданный порог, и возобновляется по команде оператора;
- сканирование прерывается при обнаружении сигнала и возобновляется после его пропадания;
- сканирование прерывается при появлении аудиосигнала и продолжается после его исчезновения;
- сканирование прерывается для анализа сигнала оператором и продолжается через некоторое время.

В современных сканерах производится запись частот сигналов в процессе сканирования.

Второй режим работы применяют для организации контроля за радиосредствами с известными частотами. При этом в некоторых образцах предусмотрено сканирование по заданному виду модуляции, а также по приоритетным каналам.

При ручном сканировании перестройка приемника осуществляется оператором, а информация выводится на жидкокристаллический дисплей. В ряде образцов на дисплее отображается относительный уровень сигналов в виде n-сегментной диаграммы.

2.3.2. Рекомендации по выбору сканирующего приемника

Приобретая сканирующий приемник, следует руководствоваться рядом практических соображений.

Чрезмерное количество каналов вызовет пропорциональное увеличение времени программирования и поиска нужного источника. Необходимое число каналов, прежде всего, зависит от исходной радиообстановки в планируемом месте применения приемника и лежит в диапазоне от 400 до 1000. При этом желательно, чтобы каналы были разделены на банки, что сделает их более доступными для поиска и упростит задачу закрепления за специальными группами источников.

Многие сканеры имеют провалы в частотном диапазоне. Не исключено, что неизвестные источники работают именно в зонах, недоступных для приема с помощью такого аппарата. Чем шире и непрерывнее диапазон рабочих частот сканера, тем более эффективно его применение.

Повышение скорости сканирования достигается введением сложнейших схем, что резко увеличивает стоимость прибора. Целесообразно применение приборов, скорость сканирования которых не пре-

вышает 50 каналов за одну секунду. Большую пользу принесет приобретение сканера, способного удерживать принимаемую частоту в течение нескольких секунд, необходимых для предварительного анализа. Тогда в случае небольшого перерыва, например при дуплексной передаче, сканер не уйдет дальше по диапазону в поисках другой рабочей частоты.

Учитывая перегрузку радиоспектра и тот факт, что условия вынуждают работать в ближней зоне излучения передатчиков, не следует стремиться к обладанию сверхчувствительным прибором, так как ничего, кроме лишних шумов в тракте, это не обещает. Чувствительность сканера выбирают, исходя из предполагаемой области его применения.

Существование многих видов модуляции сигналов вызывает необходимость остановить выбор на приборе, детектирующем сигналы с наибольшим числом модулирующих воздействий.

Очень полезной может оказаться способность прибора регистрировать уровень мощности сигнала, что позволит провести селекцию источников по удаленности от точки приема.

Наличие режима выбора приоритетного канала позволяет автоматически переходить к анализу наиболее важного источника в процессе сканирования. Если сканер будет функционировать в условиях сильных акустических шумов, следует обратить внимание на выходную мощность прибора, которая должна бытьне менее 200 мВт. Учитывая универсальность сканирующего приемника как средства обнаружения, необходимо приобретать прибор, система электропитания которого позволит эксплуатировать его в стационарных и полевых условиях.

2.4. Селективные микровольтметры, анализаторы спектра

Селективные микровольтметры представляют собой широкополосные приборы для измерения в электрических цепях уровней сигналов, а в комплекте с комбинированными антеннами — для измерения напряженности электромагнитного поля.

Ещё не столь давно наиболее широко были известны селективные микровольтметры фирмы Messelektronik Berlin:

SMV 11 — диапазон частот 9 кГц...30 МГц;

SMV 8 — диапазон частот 30...1000 МГц;

STV 301 — диапазон частот 0,1...30 МГц;

STV 401 — диапазон частот 30...300 МГц,

а также низкочастотные селективные нановольтметры:

Unipan 233 — диапазон частот 30 Гц...150 кГц;

Unipan 237 — диапазон частот 30 Гц...100 кГц.

Другую группу измерительных приборов, используемых для выявления каналов утечки информации, представляют анализаторы спектра (АС), рабочий диапазон которых достигает десятков гигагерц. Основное достоинство АС заключается в возможности наблюдать изменения панорамы радиосигналов выбранного частотного диапазона, регистрировать время появления и основные параметры.

Наиболее часто используются:

портативный анализатор Protek 3200 (30...2000 МГц);

анализаторы АРМ 723, 745, 746 (47...2050 МГц);

анализатор AVCOMPSA-65A (2...1000 МГц);

анализаторы Agilent Technologies (бывшая Hewlett-Packard) различных моделей, перекрывающих диапазон частот до 40 ГГц;

анализаторы Anritsu различных моделей, перекрывающие тот же типовой диапазон частот;

ряд анализаторов низких (звуковых) частот фирм Brüel & Kjjr, Larson Davis и Rohde & Schwarz.

Анализаторы серии АРМ фирмы Konig, предназначенные для настройки систем телевидения, обеспечивают возможность просмотра видеоизображений, а на небольших расстояниях осуществляют перехват информации с мониторов компьютеров.

При наличии соответствующих блоков такие же функции могут реализовать анализаторы фирмы Hewlett-Packard.

Анализатор спектра СК-4 «БЕЛАН 32» — это первый отечественный прибор, который по своим рабочим характеристикам не уступает импортным аналогам. Прибор имеет следующие параметры: диапазон рабочих частот 9 кГц...3,2 ГГц; стабильность опорного источника $\pm 10^{-7}$/год; измерение уровней от +30 до −135 дБм; при измерении амплитуды −135 дБм типичное соотношение сигнал-шум 15 дБ; средний уровень собственных шумов на частоте 3 ГГц: −140 дБм в полосе ПЧ 10 Гц (аттенюатор 0 дБ) и −150д Бм в полосе ПЧ 1 Гц; цифровой тракт ПЧ со значениями фильтров 1 Гц...1 МГц с кратностью шага 1, 3, 10. Фильтры ПЭМИН: 200 Гц, 9 кГц, 120 кГц; погрешность переключения фильтров 1 МГц...10 Гц не более ±0,1 дБ (для фильтров 1 Гц, 3 Гц не более ±0,25 дБ); избирательность фильтров по уровням −60/−3 дБ составляет 4:1. Уровень фазовых шумов на частоте 500 МГц при отстройке на 10 кГц составляет −110 дБн/Гц, на отстройке 1 кГц — −95 дБн/Гц, на отстройке 100 Гц — −80 дБн/Гц. С опцией 003 фазовые шумы можно снизить до значений (отстройка 100 Гц/1 кГц/10 кГц/100 кГц): −95/−107/−115/−118 дБн. Максимальный динамический диапазон свыше 100 дБ. Гарантированное значение интермодуляционных искажений третьего порядка, возникающих при подаче на вход двух равноамплитудных сигналов с уровнем −30 дБм и разносом по частоте 30 кГц не превышает −76 дБн, что

соответствует значению TOI + 8 дБм. Типичное значение интермодуляционных искажений третьего порядка: −70 дБн при подаче на вход двух сигналов −20 дБм, что соответствует значению TOI + 15 дБм. Неравномерность АЧХ для входных уровней + 10...−60 дБм во всем диапазоне частот не превышает ±0,5 дБ. Погрешность переключения аттенюатора во всем диапазоне частот ±0,7 дБ (не более ±0,5 дБ в диапазоне частот до 3 ГГц). Абсолютная погрешность измерения уровня не более ±1,5 дБ. Современное развитое меню. Широкий выбор детекторов: СКЗ, максимум, минимум, выборки, нормальный, квазипиковый. Широкий выбор демодуляторов: АМ, узкополосный ЧМ, широкополосный ЧМ. Любая размерность логарифмической шкалы: дБм, дБмВ, дБмкВ, Ватт, Вольт. Масштаб логарифмической шкалы от 20 до 0,1 дБ/деление.

Анализатор СК4-БЕЛАН 32 позволяет производить следующие автоматические измерения: мощности канала, ширины занятой полосы, мощности гармоник, глубины АМ, ЧМ девиации, коэффициента нелинейных искажений, фазовых шумов (на одной отстройке и как функции от отстройки). Возможность одновременно вывести на экран три графика: один текущий и два сохраненных. Стандартно поставляется ПО для измерения фазовых шумов. Разъем для подключения USB-носителя информации на передней панели. Встроенная ОС Windows XP. Прибор внесен в Государственный реестр средств измерений под номером 29385-05.

Рассматривая спектроанализаторы, нельзя не остановиться на последних разработках ведущих мировых компаний, а именно новой серии **спектроанализаторов реального времени RSA6100A.** Новая серия характеризуется непревзойденным сочетанием возможности отображать спектры в реальном времени, широкой полосы захвата спектра и широкого динамического диапазона, реализуя современные потребности инженеров и разработчиков в области РЧ технологий.

Специализированный видеопроцессор, построенный по технологии DPX™, обеспечивает высокоскоростной захват большого объема данных в реальном времени и построения на их базе «живой» спектрограммы, отображающей динамику измерения спектра во времени и позволяющей увидеть в динамике малейшие детали спектров и ранее недоступные для наблюдения динамичные аномалии в РЧ сигнале. Построение «живой» спектрограммы достигается кардинальным ускорением скорости захвата данных примерно в 1000 раз по сравнению с самыми быстрыми традиционными спектроанализаторами на базе качающегося фильтра или векторными анализаторами сигнала (VSA).

Тестовое оборудование для современных цифровых РЧ сигналов должно удовлетворять ряду требований: широкая полоса захвата с

хорошим динамическим диапазоном, быстрый захват сигнала и возможность строить диаграммы в осях «время – частота – модуляция». Специализированный видеопроцессор сигналов DPX осуществляет захват и обработку более 48 тысяч спектров в секунду (в обычных спектроанализаторах и векторных анализаторах — не более 50). Это обеспечивает пользователю поток информации на порядки больший, чем обеспечивают другие спектроанализаторы. Сверхбыстрый захват спектра RSA6100A позволяет получить «живой» спектр сигнала во всей динамике, а также гарантирует захват спектра сигнала, имеющего длительность от 24 мкс. Кроме «живого» отображения спектрограммы, DPX процессор позволяет отображать спектр с персистенцией (накоплением), при которой градации яркости/цвета участка сигнала соответствуют частоте его появления на экране, что гарантирует возможность зафиксировать на экране редкие аномалии, на которые глаз не успел бы среагировать. Это позволяет выделить аномалию цветом из общего потока повторяющихся спектров, ее маскирующих.

Анализаторы спектра GSP-827 (рис. 2.30) производства компании Good Will Instrument Co., Ltd. (GW Instek) внесен в Государственный реестр средств измерений и имеют следующие технические характеристики: 9 кГц... 2,7 ГГц; полоса обзора нулевая, от 2 кГц/дел до отображения всего диапазона (шаг 1-2-5); фильтры ПЧ 3/30/300 кГц/4 МГц, видео 10 Гц... 1 МГц (шаг 1-3); развертка 100 мс... 25,6 с; входной уровень $-105...20$ дБм (защита до 30 дБм, ± 25 В); аттенюатор $-30...20$ дБм; вход 50 Ом (или настраивается), КСВН $< 1{,}5$; 10 маркеров; накопление, усреднение, пиковые значения, математическая обработка, маски; память до 100 спектрограмм с временными метками; внешняя опорная частота (64 кГц/1/1,544/2,048/.../19,2 МГц); RS-232C; ЖК дисплей (640×480); универсальное питание; масса 4,5 кг. Опции: трекинг генератор; приемник AM/ЧМ/FM с выходом на наушники (jack) и динамики (3,5 мм); набор фильтров для анализа ЭМИ; GPIB; сетевой адаптер.

Рис. 2.30. Анализатор спектра GSP-827

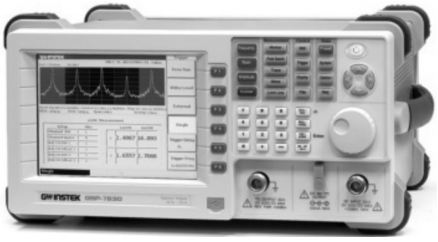


Рис. 2.31. Анализатор спектра цифровой GSP-7830

Анализатор спектра цифровой GSP-7830 (рис. 2.31) производства компании Good Will Instrument Co., Ltd. (GW Instek) внесен в Государственный реестр средств измерений под № 37467-08 и имеет следующие основные технические характеристики: частотный диапазон 9 кГц...3 ГГц; цифровая ФАПЧ; диапазон измерения уровня −122...20 дБмВт; плотность собственных шумов: −152 дБмВт/Гц (до −162 дБмВт/Гц с опцией предусилителя GAP-801); фазовый шумы −75 дБн/Гц при отстройке 20 кГц; измерение мощности в канале и соотношение мощностей в смежных каналах, измерение полосы по уровню; полоса пропускания ПЧ: 3 кГц; 30 кГц; 300 кГц; 4 МГц; маркерные измерения (10 маркеров); запись спектрограмм с временными метками (13), пределов допусков (12), пользовательских АЧХ (5), изменение последовательностей (10), профилей (10) во внутреннюю память; сохранение спектрограмм, профилей, пределов допусков, пользовательских АЧХ, изменение последовательностей, профилей настроек на USB-flash; режим Sequence: возможность программирования 10 групп последовательностей профилей и состояний (в каждой до 20 шагов); интерфейс USB, RS-232C (опция GPIB); опции: трекинг генератор, термостатированный ОГ, аккумулятор, AC/DC преобразователь, фильтры ЭМС и 300 Гц, предусилитель, демодулятор; универсальное питание: 220 В / 11...17 В (пост.); батарейное (2 шт. Li-Ion; до 3 ч) — опционально. Компактный, легкий (5 кг).

Анализаторы спектра R&S FSU (рис. 2.32) лидируют по динамическому диапазону, фазовому шуму, точности уровня и разрешающей способности — по всем параметрам, необходимым для разработки, производства и тестирования беспроводных устройств следующего поколения имеет следующие технические характеристики: диапазон частот от 20 Гц до 3,6; 8; 26,5; 43; 46 и 50 ГГц или 67 ГГц; средний уровень собственных шумов (DANL): −158 дБмВт (в полосе 1 Гц). Фазовый шум: типовое значение −133 дБн (в полосе 1 Гц) при отстройке 10 кГц. Точка пересечения по интермодуляционным составляющим 3-го порядка (TOI): типовое значение + 25 дБмВт; разрешающая способность по частоте от 1 Гц до 50 МГц; средний уровень

Рис. 2.32. Анализаторы спектра R&S FSU

собственных шумов (DANL) с предусилителем R&S FSU-B24: типовое значение −168 дБмВт (1 Гц) на частоте 20 ГГц, типовое значение −155 дБмВт (1 Гц) на частоте 50 ГГц.

Модель R&S FSU67 — первый анализатор спектра с прямым формированием диапазона частот до 67 ГГц и смешением на основной частоте: простое создание измерительной установки для диапазона частот от 20 Гц до 67 ГГц с помощью одного соединения; полноценный частотный диапазон анализа 67 ГГц; однозначная индикация частот без зеркальных каналов и комбинационных частот от внешних смесителях на высших гармониках; расширенный диапазон уровней с намного более высоким опорным уровнем, чем при использовании смесителей на высших гармониках; малая погрешность измерения уровня вплоть до 67 ГГц; низкое значение уровня собственных шумов: −152 дБмВт (1 Гц) на частоте 2 ГГц, −130 дБмВт (1 Гц) на частоте 65 ГГц. Высокая скорость измерений: быстрое измерение мощности в соседнем канале во временной области; до 70 измерений в секунду (включая передачу измерительной кривой по шине GPIB).

Большой набор возможностей: стандартные для прибора процедуры измерений: TOI (точка пересечения по интермодуляционным составляющим 3-го порядка), MC ACP(R) (мощность в соседнем канале и коэффициент мощности соседнего канала для сигналов с несколькими несущими), OBW (занимаемая полоса частот), CCDF (дополнительная интегральная функция распределения), APD (амплитудная функция распределения) и т. п. Прикладное встроенное программное обеспечение для сигналов GSM/EDGE, Bluetooth, WCDMA/HSDPA/TD-SCDMA, CDMA2000/1×EV-DV/1×EV-DO.

Поисковый анализатор спектра SpectrumJet (рис. 2.33) представляет собой полностью интегрированную систему противодействия электронному подслушиванию. Он имеет встроенные антенны и интегрированное программное обеспечение для обнаружения, анализа и поиска сигналов. По сути это портативный поисковый инструмент, с которым можно работать на ходу, не разворачивая программно-аппаратный комплекс в контролируемом помещении.

Рис. 2.33. Поисковый анализатор спектра SpectrumJet

Анализатор сканирует заданный диапазон с разрешением 10 кГц со скоростью $\geqslant$5 ГГц/с, выводя на экран полную картину спектральной плотности сигналов во всём заданном диапазоне. Сканирование может выполняться в диапазоне от 9 кГц до 21 ГГц. Специальный алгоритм обработки позволяет обнаруживать опасный сигнал, который выделяется цветом, как будто цветным маркером. Движением пальца по экрану включается «электронная лупа», с помощью которой, поворачивая прибор, ищется направление, где растёт энергетика сигнала. Возможно включение демодулятора и коррелятора, что позволит оперативно определить принадлежность и характер обнаруженного сигнала.

Встроенная антенная система, установленное программное обеспечение, простое управление делают прибор оптимальным для решения оперативных задач по защите от утечек информации по радиоканалу. Анализатор может воспроизводить спектральную панораму во всём диапазоне. Участок с обнаруженным сигналом просматривается с помощью «электронной лупы» без остановки сканирования. Воспроизведение диаграммы время-частота (водопада) возможно одновременно со спектром, так же, как и листинг новых сигналов. Имеется набор стандартных демодуляторов с различными полосами приёма. Специальное меню позволяет перейти в режим контроля сотовой телефонии и беспроводного доступа.

Высокая скорость анализа даёт возможность наблюдать «живой эфир» — весь диапазон контроля на экране, обновляющийся практически ежесекундно. Программное обеспечение RSSpectrum позволяет мгновенно фиксировать и наблюдать новые источники сигналов. Высокая скорость анализа позволяет накапливать и усреднять большое число реализаций за считанные секунды, что существенно повышает вероятность обнаружения шумоподобных и широкополосных сигналов. Также анализатор упрощает обнаружение сигналов со скачками по частоте (FH или ППРЧ) и коротких сигналов (burst).

Анализатор SpectrumJet благодаря высокой скорости анализа позволяет увидеть и сотовые телефоны, и доступ через Wi-Fi или LTE. Понаблюдайте, накопите реализации и научитесь различать внутренние источники от внешних. Стандартные же связные сигналы и сигналы радио и телевещания не будут мешать вам постоянным мельканием на экране.

SpectrumJet разработан специально для оперативного поиска несанкционированных передатчиков внутри помещений или на открытых площадках, зонах и т. д. Программное обеспечение специально написано под управление приемником через touch screen. Например, для пользования лупой при рассмотрении детального спектра сигнала достаточно провести пальцем справа налево по интересующему участку панорамы.

Кроме того, поисковый анализатор спектра SpectrumJet может быть использован для проведения радиомониторинга в заданном районе и решения задач радионаблюдения, радиоразведки и контроля каналов утечки информации. Программное обеспечение позволяет вести статистическую обработку сигналов за время предыдущего наблюдения, классифицировать сигналы и обнаруживать новые на фоне ранее накопленной усредненной панорамы. Отметим, что все перечисленные операции осуществляются теперь гораздо быстрее.

Опционально анализатор может быть дополнен набором датчиков для анализа сигналов в сети электропитания, в проводных линиях и в оптическом диапазоне, а также набором видеодетекторов. Управление анализатором осуществляется непосредственно с экрана (touch screen). Установленное программное обеспечение обеспечивает работоспособность анализатора не только в режиме анализа спектра, но и в режимах радиомониторинга и ручного управления. Программное обеспечение даёт возможность проводить анализ спектральных характеристик и соответствующие измерения, не прерывая процесс мониторинга. Для регистрации и демодуляции обнаруженного сигнала следует использовать ручной режим.

2.5. Автоматизированные поисковые комплексы

Выявление активных средств негласного съема акустической информации (радиомикрофонов, микрофонов с передачей информации по электросети переменного тока, радиотрансляционным и другим проводным сетям, телефонных передатчиков с передачей информации по радиоканалу, радиостетоскопов и др.), локализация их местоположения в пределах контролируемого помещения является первоочередной задачей служб безопасности по защите информации.

Другим важным направлением деятельности являются: постоянный или периодический контроль загрузки радиодиапазона, выявле-

ние и анализ новых излучений, оценка их опасности для учреждения, выявление потенциальных и специально организованных радиоканалов утечки информации (например, цифровых радиозакладочных устройств или устройств с накоплением и последующей передачей).

Каждая из этих задач — многоэтапная, решается в условиях сложной электромагнитной обстановки как на объектах, так и на выезде, и требует широкой номенклатуры специальных технических средств. Эти средства должны обеспечивать:

- обнаружение за минимальный интервал времени устройств активного съема акустической информации и определение их местоположения;
- панорамный анализ широкого диапазона частот в реальном времени в условиях сложной электромагнитной обстановки, оценку параметров излучений, адаптацию к окружающей радиообстановке, выявление и анализ ее изменений;
- протоколирование (регистрацию) в течение длительного времени амплитудно-частотно-временной загрузки исследуемого диапазона с привязкой к реальному времени;
- статистический анализ зарегистрированных данных загрузки диапазона с возможностью протоколирования интегральных показателей по каждому радиоканалу (источнику), сравнение с базами данных и выявление корреляционных частотно-временных взаимосвязей радиоканалов.

Для решения приведенных задач в последнее время все чаще используются автоматизированные аппаратно-программные комплексы ближней радиоразведки, которые позволяют автоматизировать весьма трудоемкие и требующие достаточно высокой квалификации персонала операции по обнаружению, идентификации и локализации источников несанкционированного радиоизлучения.

В простейшем случае такой комплекс может состоять из стандартного сканирующего приемника, управляемого ПЭВМ, работающей под управлением специального программного обеспечения. Более сложные системы также построены на базе управляющей ПЭВМ, сканирующего приемника, в большинстве случаев модернизированного, а в последнее время специально разработанных различных дополнительных блоков, повышающих быстродействие (блоки аналогово-цифровой обработки, блоки быстрого преобразования Фурье (БПФ) и т. д.). Они существенно расширяют функциональные возможности комплекса (аппаратные корреляторы, контроллеры, внешние микрофоны и т. п.).

Достоинствами таких комплексов являются сравнительно невысокая стоимость, модульная организация аппаратной части, допускающая простую модернизацию (замена отдельных функциональных

блоков). Малый вес и сравнительно небольшие габариты в сочетании с универсальным питанием (220 В, 12 В) и встроенными аккумуляторными батареями позволяют эксплуатировать комплексы как в стационарных, так и в полевых условиях.

2.5.1. Принципы функционирования комплексов

Начальным этапом функционирования автоматизированного аппаратно-программного комплекса является адаптация к окружающей электромагнитной обстановке. На данном этапе автоматически формируется так называемый «исходный файл», в который заносится амплитудно-частотная загрузка рабочего диапазона вне контролируемого помещения. Исходный файл рекомендуется получать сканированием частотного диапазона в районе проверяемых помещений на удалении от них на 300...500 м, но не более 1000 м. Выполнение данной операции позволяет впоследствии значительно ускорить обнаружение и анализ «неизвестных» сигналов в контролируемом помещении.

На этапе поиска несанкционированных передающих устройств персональный компьютер перестраивает сканирующий радиоприемник в заданном диапазоне частот и на каждом шаге перестройки сравнивает уровень принимаемого сигнала с установленным порогом. В случае превышения порога несущая частота обнаруженного источника излучения измеряется и записывается в память. Для обнаруженного сигнала компьютером может проверяться предположение о том, что источником излучения является находящийся в помещении радиомикрофон. Проверка, как правило, выполняется по следующим признакам:

- обнаруженный сигнал не содержится в списке «Известных» компьютеру;
- обнаруженный сигнал имеет вторую или третью гармоники (что характерно для некоторых близко расположенных миниатюрных радиопередатчиков раннего поколения);
- обнаруженный сигнал модулируется звуковыми сигналами, воспроизводимыми в помещении (что характерно для ЗУ с открытым каналом передачи);
- спектральные характеристики сигнала изменяются при изменении акустического фона в помещении;
- сравнение уровня принимаемого сигнала от «опорной» (размещенной вне контролируемого помещения) и «рабочей» (находящейся в контролируемом помещении) антенн.

Оператор обычно имеет возможность настраивать специальное программное обеспечение таким образом, чтобы проверка обнаруженного излучения выполнялась сразу по всем этим признакам или только по некоторым из них.

Для проверки по первому признаку необходимо предварительно собрать данные о внешних излучениях (сформировать «исходный файл»). Проверка по второй и третьей гармоникам выполняется автоматической настройкой приемника на частоту, соответственно в два или три раза большую несущей частоты обнаруженного излучения.

Окончательная идентификация излучений на принадлежность к классу радиомикрофонов осуществляется на основе взаимной корреляционной обработки демодулированного сигнала со специальным зондирующим акустическим сигналом, излучаемым размещённой в контролируемом помещении акустической системой (активное тестирование) или с использованием акустического фона помещения (пассивное тестирование).

Для определения местоположения выявленной закладки раньше чаще всего использовался метод акустической локации. В процессе акустической локации акустические системы, встроенные либо подключаемые к комплексу, излучают тестовый сигнал (обычно напоминающий щелчки импульса). По задержке звукового сигнала, принятого по радиоканалу относительно излученного, определяются расстояния от каждой из колонок акустической системы до обнаруженного радиомикрофона. При надлежащем выборе мест размещения колонок программа компьютера позволяет определить координаты источника излучения на экране монитора как точку пересечения окружностей с радиусами, равными измеренным расстояниям. До недавнего времени большинство комплексов оснащалось акустической системой, состоящей из двух колонок, позволявшей провести локализацию местоположения закладки только в одной плоскости. При необходимости определения координат закладочного устройства в трехмерном пространстве контролируемого помещения необходимо провести как минимум два теста: первый — располагая колонки акустической системы в горизонтальной плоскости, второй — колонки акустической системы располагаются в вертикальной плоскости. Точность определения местоположения закладки напрямую зависит от местоположения и ориентации акустических систем и увеличивается с ростом числа проведенных акустических тестов.

В настоящее время в связи с более активным использованием закладочных устройств с различными видами закрытия канала передачи (различные частотные манипуляции, дельта модуляция, ППРЧ и т. д.) изложенным выше методом акустической локации можно определить местонахождение закладочных устройств только с открытым каналом передачи данных.

Альтернативой методу акустической локации в настоящее время служит метод сравнения уровней сигнала, излучаемого закладочным устройством и принимаемого с нескольких антенн, установленных

в контролируемых помещениях. Для использования данного метода комплекс оснащается управляемым коммутатором для подключения распределенной антенной системы. В задачу данного метода не входит точное определение местоположения закладки. С использованием данного метода оператор, с высокой степенью вероятности, дает ответ о нахождении закладочного устройства в конкретном помещении. Данный метод является более эффективным при обнаружении современных закладочных устройств, хотя и требует выполнения некоторых обязательных условий, а именно:

- базовая антенна от рабочих антенн должна отделяться капитальными перегородками или выноситься на чердачное помещение;
- соединение антенного коммутатора с рабочими и базовыми антеннами должно выполняться кабелями одной длины и с низким погонным затуханием.

2.5.2. Специальное программное обеспечение

Ядром современных аппаратно-программных комплексов является специальное программное обеспечение (СПО), предназначенное для автоматического управления сканирующим приемником, проведения автоматического анализа радиосигналов в контролируемом помещении и выдачи результатов оператору.

Существующее в настоящее время СПО по функциональным возможностям можно разделить на две группы:

- программное обеспечение, предназначенное для решения задач радиомониторинга и исследования радиосигналов;
- универсальное программное обеспечение, обладающее рядом специальных программных инструментов для исследования сигналов и поиска закладочных устройств.

Выбор программного обеспечения, на базе которого будет построен автоматизированный комплекс, обычно производится исходя из условий конкретного комплекса задач.

Для решения спектра задач, связанных с обнаружением, анализом и контролем радиосигналов, целесообразно использовать СПО, предназначенное для проведения радиомониторинга. Особенностью такого СПО является возможность проводить автоматизированный дискретно-шаговый радиоконтроль фиксированных частот и полос частот в заданных границах для обработки и анализа сигналов, а также отображения, регистрации, документирования и хранения полученной информации.

В том случае, если основной задачей создаваемого комплекса будет обнаружение факта утечки информации, необходимо, чтобы используемое СПО позволяло обнаруживать новые радиосигналы, проводить их идентификацию и при необходимости анализировать об-

наруженный сигнал с использованием дополнительных программных инструментов.

Для проведения наиболее полного комплекса работ по выявлению, исследованию и локализации подслушивающих устройств программное обеспечение должно обладать набором программных инструментов, которые позволили бы проводить всесторонний анализ обнаруженных сигналов, а также имели бы возможность определения местоположения найденных закладочных устройств. Важной особенностью программного обеспечения является возможность использования дополнительных (вспомогательных) аппаратных средств для решения поставленной задачи.

В настоящее время на российском рынке подавляющее число фирм, занимающихся разработками поисковых комплексов, реализуют СПО совместно с аппаратной частью комплекса, не раскрывая его содержания. Достаточно сложно получить достоверную информацию о структуре программного обеспечения и только некоторые фирмы реализуют программное обеспечение, позволяющее построить самостоятельно недорогой комплекс. Примером такого программного обеспечения является универсальные программы обнаружения средств негласного съема информации серии «Филин», предназначенные для создания на их основе аппаратно-программных комплексов поиска и локализации средств негласного съема акустической информации (в том числе видеокамер, передающих информацию по радиоканалу). Для создания программно-аппаратного комплекса в качестве аппаратных средств достаточно иметь любой сканирующий приемник из широкой номенклатуры радиоприемных средств фирм ICOM, AOR Co. Ltd или WiNRADiO и звуковую карту. Кроме того, при желании в качестве дополнительных аппаратных средств могут использоваться анализаторы спектра (серии 859... фирмы Agilent Technologies) или специально разработанные устройства быстрого панорамного анализа (аналоги анализатора спектра). В этом случае скорость и качество поиска существенно возрастают. Программа «Филин» обеспечивает управление аппаратными средствами, съем, хранение, обработку и представление данных.

Программа работает под управлением операционных систем начиная от Windows 2000-XP.

Базовым требованием к разрешающей способности экрана является разрешение 1024×768 точек и палитра 16 или более битов глубины цвета (65535 цветов). Работа при более низком разрешении возможна, однако при этом эргономические показатели по детализации представляемой информации будет ниже, чем при базовом разрешении экрана.

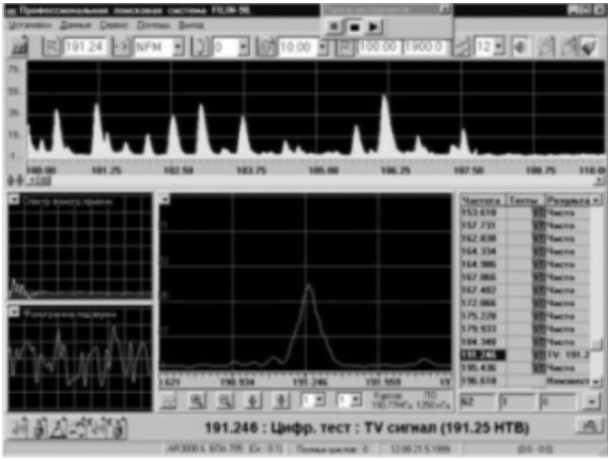


Рис. 2.34. Вид экрана монитора с тестовым ТВ сигналом

Звуковая карта необходима для записи демодулированного аудиосигнала с выхода приемника и для тестирования сигнала в поисковой версии. Для мониторинговых задач достаточно иметь звуковую карту, которая корректно работает в среде Windows (записывает и воспроизводит аудиосигналы стандартными мультимедиа программами). Для корректной работы программы в поисковой версии к звуковой карте предъявляются дополнительные требования:

- звуковая карта должна быть полнодуплексной;
- звуковая карта должна иметь микрофонный или линейный стереовход;
- проникновение сигнала из канала в канал должно быть минимальным.

В программе реализовано большинство из известных в настоящее время алгоритмов обнаружения радиоизлучающих закладочных устройств, в частности алгоритмов, используемых в комплексах OSCOR 5000, АРК-Д1, АРК-Д3, RS-1000 и других. Это обеспечивает относительно высокую вероятность обнаружения средств негласного съема информации при низком уровне ложной тревоги.

Важной особенностью программы «Филин» является воплощение концепции единого рабочего экрана, содержащего в себе всю необходимую информацию (рис. 2.34). Это избавляет пользователя от необходимости открывать иерархическую систему окон и повышает эффективность работы.

Для идентификации радиоизлучающих закладочных устройств в программе предусмотрено до восьми одновременно используемых прогрессивных алгоритмов обнаружения. Результат выполнения каж-

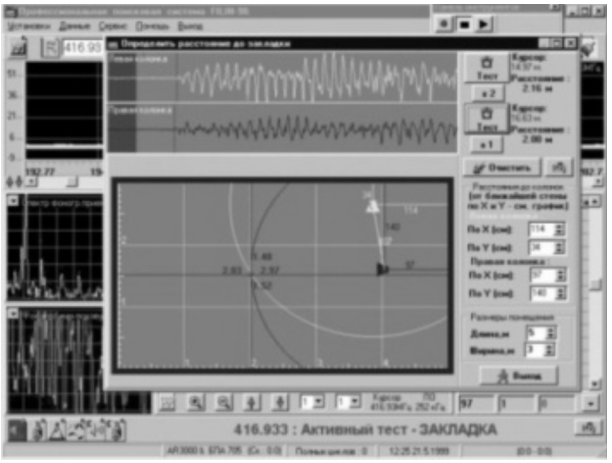


Рис. 2.35. Вид экрана монитора при обнаружении ЗУ

дого из тестов несет в себе полную информацию о наличии или отсутствии закладочного устройства (рис. 2.35).

Комплексное использование тестов позволяет добиться гораздо большей вероятности обнаружения при меньшей вероятности ложной тревоги. Имеется возможность автоматической классификации цифровых каналов передачи данных, что существенно облегчает обнаружение цифровых радиомикрофонов.

Программа без участия оператора осуществляет все необходимые для оптимального решения задачи действия и функции управления вплоть до представления конечных результатов, оставляя для пользователя только функцию первоначального определения конфигурации. Это дает возможность даже не очень квалифицированному оператору получать надежные и достоверные результаты.

Реализованные в программе алгоритмы получения, хранения, обработки и представления данных позволяют оператору при необходимости в экспертном режиме проводить анализ радиосигналов. Это дает возможность оператору выявлять любые типы радиоизлучающих средств негласного съема информации вне зависимости от алгоритма их функционирования и вида модуляции (в том числе с накоплением информации, с перестраиваемой рабочей частотой, сложной модуляцией и т. д.).

Протокол, в котором фиксируются все события, связанные с контролем радиоэфира, и визуализированные из базы данных изображения панорам радиосигналов будут служить документальным подтверждением выводов, сделанных оператором.

Удобный пользовательский интерфейс, высококачественное представление графических и цифровых данных в максимальной степени

облегчают работу с использованием универсальной программы «Филин».

Для построения специализированного аппаратно-программного комплекса «Касандра» используется СПО Inspector. Это комплекс измерительных и управляющих программ. Данные программы предназначены: для обеспечения эффективного и высокоскоростного процесса инструментального контроля радиочастотного спектра, выполнения метрологически аттестованных измерений радио- и радиотехнических параметров излучений, долговременного контроля радиочатотного спектра, сбора, хранения, обработки и представления результатов измерений, решения ряда специализированных задач с помощью анализаторов спектра и измерительных приемников.

Специальное программное обеспечение Inspector состоит из ряда программ, решающих отдельные функциональные задачи. Отдельные программы могут взаимодействовать друг с другом при передаче данных и управления, при этом расширяются их функциональные возможности.

Основной принцип, заложенный в СПО Inspector: все результаты измерений спектров сигналов и диапазонов частот сохраняются в файлах баз данных. Ограничений на максимальное время сканирования (объем сохраненной информации) в алгоритмах СПО нет. Единственным ограничением на объем хранимых данных (времени сканирования) является емкость жесткого диска. При применении жесткого диска емкостью 80...100 Гбайт время непрерывной работы анализатора спектра может достигать нескольких месяцев. Используемые в СПО алгоритмы удаления невостребованных файлов баз данных результатов измерений практически позволяют снять ограничение на максимальное время работы СПО.

С помощью сохраненных результатов измерений спектров и панорам можно провести экспертный анализ состояния радиочастотного спектра, выполнить ряд измерений в отложенном режиме.

Данный подход гарантирует, что ни одно, даже самое кратковременное событие, зафиксированное анализатором спектра, не будет потеряно. Следовательно, результаты измерений состояния радиочастотного спектра в любом частотно-временном интервале можно будет детально исследовать с помощью программы постобработки.

Программа InspectorRC применяется в случае, когда оператору необходимо решать задачи, связанные с контролем одного или нескольких диапазонов частот. Задание контроля для данной программы ставится следующим образом: необходимо сканировать определенный диапазон частот, определенный начальной и конечной частотой сканирования с определенным шагом по частоте (разрешением).

При выполнении одного сканирования от начальной до конечной частоты анализатор спектра может несколько раз перестраиваться по частоте. За одно измерение анализатор спектра охватывает диапазон частот $\Delta F = S_{\text{пер}}(N-1)$, где ΔF — охватываемый анализатором спектра диапазон частот или полоса обзора; $S_{\text{пер}}$ — заданный шаг перестройки (разрешение по частоте), шаг перестройки не может превышать полосу пропускания; N — количество точек в графике анализатора спектра.

Если охватываемый анализатором спектра диапазон частот меньше заданного в задании, то анализатор спектра перестраивается на частоту, обеспечивающую сканирование следующего поддиапазона частот. Этот процесс повторяется до тех пор, пока не будет достигнута верхняя заданная частота сканирования.

Программа InspectorRT применяется для исследования диапазона (диапазонов) частот на наличие дополнительных излучений. Под дополнительными излучениями понимаются побочные излучения радиоэлектронных средств, излучения незаконно действующих передатчиков (НДП), любые другие излучения, наличие которых в радиоэфире не регламентировано, нежелательно или представляет опасность (например, закладных устройств). Также с помощью программы InspectorRT можно выполнять исследование и инженерный анализ радио- и радиотехнических параметров отдельных излучений. Принятие решения о наличии опасных сигналах осуществляется по результатам анализа амплитудно-частотно-временного представления графиков панорам, что позволяет наблюдать временные изменения в параметрах излучений, выявлять характерные демаскирующие признаки работы передатчиков, имеющих сложные алгоритмы работы (маскировки) во времени. Выполняется сохранение всех результатов измерений электромагнитного поля в анализируемом диапазоне частот для отложенного анализа и получения экспертного заключения, объективного контроля выполненных работ, создания архивов результатов контроля важных технических средств и объектов, пополнения базы данных с демаскирующими признаками опасных сигналов. Формируется список опасных сигналов с возможностью последующего анализа данного списка. Поиск опасных сигналов выполняется следующими методами: методом разности панорам (в том числе с использованием антенного коммутатора), методом сравнения с порогом, метод сравнения с эталонной панорамой.

2.5.3. Специализированные поисковые программно-аппаратные комплексы

Специализированные поисковые программно-аппаратные комплексы предназначены для автоматического поиска радиоизлучающих

подслушивающих устройств, в большинстве случаев обладают повышенной производительностью и снабжены рядом дополнительных сервисных функций.

Основной характеристикой для таких комплексов является показатель производительности: скорость панорамного анализа загрузки радиодиапазона с учетом времени, затрачиваемого комплексом на надежное определение принадлежности обнаруженного сигнала к классу сигналов подслушивающих устройств.

Производительность комплексов особенно важна, если речь идет об обнаружении дистанционно управляемых или кратковременно излучающих радиозакладок, а также в случае необходимости немедленной нейтрализации канала возможной утечки конфиденциальной акустической информации (например, при включении микрофона, принесенного кем-либо из участников совещания или конфиденциальных переговоров).

С учетом приведенных выше соображений существующее многообразие поисковых комплексов может быть сведено к двум основным группам: с обычной и высокой производительностью.

К первой группе следует отнести комплексы, производительность которых определяется, главным образом, технической скоростью сканирования используемых радиоприемников (в том числе создаваемые пользователями с использованием сканирующего радиоприемника, ПЭВМ и специального программного обеспечения).

Ко второй группе могут быть отнесены более сложные и, соответственно, более дорогие комплексы, в состав которых входит специальная аппаратура для повышения скорости панорамного анализа.

Помимо приведенных выше характеристик весьма значительным является наличие либо отсутствие возможности проведения оператором анализа динамических характеристик обнаруживаемых сигналов вручную в реальном времени. Это принципиально важно для детального анализа акустически некоррелируемых сигналов, относимых к вероятным сигналам от радиозакладок, и принятия оператором правильного решения о принадлежности анализируемого сигнала средству съема конфиденциальной информации.

Все вышесказанное справедливо и для мобильных вариантов поисковых комплексов, которые раньше использовались для контроля только одного помещения в текущий момент времени. В большинстве случаев такие комплексы конструктивно выполнены в кейсе и имеют возможность автономного питания, что позволяет использовать их в полевых условиях.

Для обеспечения безопасности объектов, представляющих собой несколько пространственно разнесенных помещений или целое здание, как правило, используются многоканальные варианты поисковых

комплексов, которые позволяют вести одновременный непрерывный радиоконтроль всех зон безопасности.

Такие комплексы имеют распределенную антенную систему, в состав которой входит опорная антенна, обычно устанавливаемая на крыше здания, и несколько малогабаритных широкополосных рабочих антенн. Ядром комплекса является единый центр управления, в котором размещаются управляющая ПЭВМ, сканирующий приемник и коммутационное оборудование.

Основные функциональные характеристики многоканальных стационарных систем радиоконтроля мало отличаются от характеристик современных мобильных комплексов.

Очевидно, что для непрерывного анализа обстановки в нескольких пространственно разнесенных помещениях по радиоканалу и в каналах иной природы (например, проводных сетях) необходимо наличие эффективных алгоритмов поиска, идентификации, анализа и регистрации сигналов, а также средства ускоренного сканирования радиодиапазонов. Дополнительное аппаратное и программное обеспечение должно обладать достаточной гибкостью, чтобы упростить создание и модернизацию системы в соответствии с текущими потребностями пользователя.

Обнаружение сигналов в проводных сетях. Для обнаружения и идентификации сигналов в проводных сетях в автоматизированных поисковых комплексах обычно используются конвертеры, подключаемые к антенному входу сканирующего приемника.

Конвертер содержит схему подключения к электросети с гальванической развязкой, фильтры подавления помех, а также смеситель и гетеродин с кварцевой стабилизацией частоты.

Принцип функционирования основан на переносе полосы частот проводного канала (0,01...5 МГц) в УКВ диапазон, обычно в диапазон 40...45 МГц либо 60...65 МГц. Частота сигнала в сети электропитания или другом проводном канале определяется как разность между частотой настройки приемника и частотой гетеродина конвертера. При применении дополнительных зондов появляется возможность обнаружения сигналов, передаваемых в оптическом (инфракрасном) диапазоне.

В процессе анализа проводных линий могут использоваться все базовые операции сканирования, обнаружения, идентификации и локализации.

Нейтрализация обнаруженных радиомикрофонов. Для оперативной нейтрализации радиомикрофонов, выявленных в контролируемом помещении, могут использоваться программируемые генераторы прицельной помехи.

Типовой генератор прицельной помехи содержит цифровой синтезатор частоты, широкополосный усилитель мощности, генератор модулирующего псевдошумового сигнала, схему интерфейса и встроенный импульсный источник питания. Схема интерфейса принимает данные от персонального компьютера или коммутирующего устройства (микроконтроллера) через параллельный порт или по последовательной шине и преобразует их в коды управления частотой синтезатора. Модулирующий сигнал представляет собой импульсную псевдошумовую последовательность с тактовой частотой около 600 кГц и периодом от 1,2 до 0,3 кГц.

Генератор имеет два режима работы:

- автономный — управление и настройка на рабочую частоту осуществляется пользователем с помощью соответствующего программного обеспечения;
- автоматический — полное управление генератором осуществляет программное обеспечение поискового комплекса.

В автоматическом режиме производятся следующие базовые операции: включение и настройка генератора на частоту обнаруженного излучения, которое идентифицировано комплексом как сигнал радиомикрофона. Если таких сигналов несколько, несущая частота генератора последовательно переключается для нейтрализации всех одновременно функционирующих передатчиков. В последнем случае эффективная мощность помехи уменьшается пропорционально числу таких частот. В нижней половине рабочего диапазона генератор помимо основной частоты излучает гармоники, уровни которых на 10...20 дБ ниже несущей. В результате излучение радиомикрофона будет нейтрализовано не только на несущей частоте, но и на ее гармониках.

2.5.4. Мобильные поисковые комплексы

Комплекс обнаружения радиоизлучающих средств и радиомониторинга «Крона-плюс» (рис. 2.36) предназначен для обнаружения и локализации средств негласного съема информации, передающих данные по радиоканалу (радиомикрофонов, радиостетоскопов и др.), использующих все известные на сегодняшний день способы маскирования сигналов, в диапазоне рабочих частот при анализе радиочастотного спектра: 0,01...3000 МГц (до 6000 МГц с дополнительным конвертором ПС-6000 или до 9000 МГц с дополнительным конвертором ПС-9000). Позволяет обнаружить радиосигналы, модулированные по амплитуде или частоте акустическим сигналом, а также ряд радиосигналов с закрытием речи (инверсия спектра, отдельные цифровые алгоритмы передачи аудиоданных); радиосигналы со сложными алгоритмами закрытия речи и другие источники радиоизлучений в контролируемом помещении (обнаруживаются и локализуются с помощью

Рис. 2.36. Комплекс обнаружения радиоизлучающих средств и радиомониторинга «Крона-плюс»

специальных методик). Максимальная дальность при автоматизированной локализации 20 м. Мощность излучения обнаруживаемых радиомикрофонов более 50 мкВт. Ошибка при определении дальности до радиоизлучающего подслушивающего устройства ≈10 см.

С помощью комплекса можно решать широкий круг задач радиомониторинга. Он позволяет с высоким быстродействием определить параметры радиосредств в диапазоне до 3 ГГц (до 9 ГГц с дополнительным конвертором), сохранить их в базе данных, распознать скрытно установленные в помещении радиомикрофоны и определить расстояние до них. Имеет возможность автоматического распознавания цифровых каналов передачи данных, а также обнаружения скрытых видеокамер, передающих информацию по радиоканалу. Комплекс реализует наиболее передовые алгоритмы обнаружения подслушивающих устройств. Применение до восьми алгоритмов обнаружения, каждый из которых базируется на использовании различных индивидуальных демаскирующих признаков подслушивающих устройств, позволяет с высокой достоверностью выявлять наличие любых радиомикрофонов, в том числе с маскировкой сигналов как по алгоритмам модуляции, так и по способам их передачи (закладочные устройства с цифровыми каналами передачи данных, с накоплением информации, с перестраиваемой рабочей частотой и т. д.).

Основным отличием комплекса «Крона-плюс» от изделия «Крона» является включение в его состав блока быстрого панорамного анализа. Это позволило повысить скорость обзора диапазона до 100 МГц/с и существенно увеличить вероятность обнаружения комплексом коротких сигналов (как однократных, так и периодически появляющихся в эфире). Тем самым заметно улучшены характеристики комплекса по оперативности выявления радиоизлучающих закладочных устройств со скачкообразным изменением (псевдослучайной перестройкой) рабочей частоты, а также устройств с накоплением информации и её передачей в режиме быстродействия.

Комплекс предназначен как для экспресс-анализа наличия радиоизлучающих подслушивающих устройств в контролируемом помещении, так и для долговременного круглосуточного мониторинга электромагнитной обстановки в одном или нескольких контролируемых

помещениях. Применяемые алгоритмы сбора, обработки и представления статистической информации, удобный графический интерфейс программного обеспечения в сочетании со специальными методиками обнаружения позволяют с высокой вероятностью выявлять несанкционированные излучения из контролируемого объекта.

Широкие возможности программного обеспечения (опция «Филин-ультра») позволяют применять комплекс для решения основных задач радиомониторинга: поиска и оценки параметров новых или известных сигналов, контроля диапазона частот, контроляфиксированных частот и т. д. Программное обеспечение позволяет при обнаружении сигнала автоматически определять его параметры и записывать их в базу данных. Имеется возможность заранее запрограммировать автоматическое проведение и других действий, необходимых при решении отдельных задач. Использование дополнительного конвертора позволяет провести исследование как радиоэфира, так и проводных линий с анализом низкочастотных сигналов. Возможна эксплуатация комплекса в различных конфигурациях при оснащении дополнительным оборудованием: антенно-фидерными устройствами, СВЧ преобразователями частоты, антенными коммутаторами, сетевыми адаптерами для подключения к сети электропитания и проводным линиям, генераторами для оперативного блокирования выявленных каналов утечки информации. При использовании блока быстрого панорамного анализа скорость обзора увеличивается до 100 МГц/с. Применение различных конверторов позволяет расширить диапазон контроля до 9000 МГц или исследовать низкочастотные сигналы в электросети 220 В, телефонной линии и ИК диапазоне (с дополнительным зондом).

Большинство возможностей комплекса реализуется программным обеспечением, которое постоянно совершенствуется. Новые версии программного обеспечения разрабатываются с учетом совместимости со старыми версиями, что позволяет наращивать возможности комплекса при минимальных издержках.

Автоматизированные мобильные комплексы радиоконтроля RS digital Mobile 7G, RS digital Mobile 12G (рис. 2.37) предназначены для проведения радиомониторинга в заданном районе и могут быть использованы для задач радионаблюдения, радиоразведки и контроля каналов утечки информации в диапазоне частот от 9 кГц до 7 ГГц (12 ГГц для RS digital Mobile 12G); коэффициент шума не более 6 дБ; динамический диапазон не менее 70 дБ; уровень побочных продуктов (spurious) при включенном на входе 50-омном эквиваленте не более −115 дБм; полоса анализа 400 кГц; разрешение по частоте в режиме мониторинга 12,5 кГц; разрешение по частоте в режиме векторного анализатора спектра 0,78 кГц; время расчета комплексного спектране

Рис. 2.37. Автоматизированный мобильный комплекс радиоконтроля RS digital Mobile 7G (RS digital Mobile 12G)

более 150 мкс; время анализа диапазона 100 МГц...7 ГГц не более 5,5 мин; диапазон регулировки цифрового АРУ 110 дБ.

В комплексах используется система цифровой обработки сигналов (ЦОС) на базе процессора DSP56803 фирмы Motorola, позволяющая осуществлять векторный анализ сигналов на выходе ПЧ радиоприемного тракта. Программное обеспечение RS digital позволяет вести статистическую обработку сигналов за время предыдущего наблюдения, классифицировать сигналы и обнаруживать новые на фоне ранее накопленной усредненной панорамы. С использованием системы ЦОС программа позволяет наблюдать тонкую структуру сигнала с разрешением до 0,78 кГц. Комплексы содержат встроенный СВЧ конвертер, переносящий сигналы из диапазона 2...7 ГГц в диапазон 0,5...2 ГГц, содержащий 4 фильтра с полосой пропускания 1,0...1,5 ГГц, что обеспечивает достаточное подавление зеркального канала. Конструктивно комплексы расположены в ударопрочных герметичных кейсах Peli-1520. Управление комплексами осуществляется по шине USB от портативного компьютера с процессором не ниже Pentium-IV 1,7 ГГц, входящего в комплект поставки.

В состав комплексов входят комплекты антенн: широкополосная рамочная антенна RS/A для диапазона 50...2000 МГц; изотропная антенна на малогабаритном штативе RS/A/2-12 для диапазона 2... 12 ГГц.

Опционально комплексы могут быть дополнены: генераторами RS/N с антенной SI-5002.1 для оперативного подавления сосредоточенной помехой несанкционированного источника излучений в диапа-

зоне 89...1800 МГц (30...2000 МГц); НЧ конвертерами RS/L plus для анализа сигналов как в эфире, так и в проводных линиях, либо в оптическом диапазоне;направленной антенной RS/A/0,5-12 диапазона 0,5...12 ГГц (сертификат соответствия имеется, КСВ антенны менее 1,5 во всем диапазоне).

В состав комплекса входит комплект антенн:

- широкополосная рамочная антенна RS/A для диапазона 50... 2000 МГц;
- изотропная антенна на малогабаритном штативе RS/A/2-12 для диапазона 2...12 ГГц.

Опционально комплекс может быть дополнен:

- генератором RS/N с антенной SI-5002.1 для оперативного подавления сосредоточенной помехой несанкционированного источника излучений в диапазоне 89...1800 МГц (30...2000 МГц);
- НЧ конвертером RS/L plus для анализа сигналов как в эфире, так и в проводных линиях, либо в оптическом диапазоне;
- направленной антенной диапазона 0,5...12 ГГц (сертификат соответствия имеется, КСВ антенны менее 1,5 во всем диапазоне). Наличие шины I2C позволяет подключать к комплексу любые аксессуары, производимые компанией.

2.5.5. Стационарные комплексы автоматизированного обнаружения радиомикрофонов

Предназначены для защиты объекта, представляющего несколько пространственно разнесенных помещений, от угроз, связанных с несанкционированной передачей информации подслушивающими устройствами или другими радиоэлектронными средствами.

В принципе, для проведения периодического радиоконтроля нескольких зон безопасности можно использовать один мобильный комплекс поиска подслушивающих устройств. Однако для достоверного выявления эпизодически функционирующих радиосредств, например дистанционно управляемых, радиоконтроль во всех зонах необходимо вести непрерывно.

Кроме того, в обязанности системы радиоконтроля может входить наблюдение за радиообстановкой вблизи объекта, а также анализ сигналов и выявление несанкционированных передач в проводных коммуникациях и оптическом (инфракрасном) канале.

Таким образом, система комплексного радиоконтроля должна непрерывно анализировать данные радионаблюдения, поступающие по нескольким каналам различного вида, причем с ростом каналов скорость сканирования, по сравнению с одноканальным вариантом, не должна заметно уменьшаться.

Принципы построения таких комплексов могут быть различны, рассмотрим наиболее типичны.

Комплекс с распределенной антенной системой и единым центром управления. Достоинствами систем такого типа являются легкая модифицируемость и наращиваемость, удобство управления, высокая надежность. К недостаткам данной системы можно отнести сложность первоначального монтажа, ограниченность расширения системы (обычно контролирует от 21 до 23 помещений), снижение скорости обработки результатов при значительном увеличении количества помещений. Типичными представителями комплексов данного вида являются комплексы RS1100 и АРК-Д3-12.

Комплексы, состоящие из центра управления, в котором размещается управляющая ПЭВМ с коммутационным оборудованием, и установленные в контролируемых помещениях дистанционно управляемые сканирующие приемники. Управление сканерами может проводиться как с помощью специально проложенных коммуникаций, так и по локальной сети. К достоинствам данной системы можно отнести отсутствие значительного снижения скорости обработки информации при увеличении количества контролируемых помещений. Недостатком данных систем является сложность и ограниченность (до 10 контролируемых помещений) расширения системы. Типичными представителями комплексов, построенных по данному принципу, являются комплексы серии «Дельта».

Автоматизированный комплекс пространственно-распределенного радиоконтроля RS1100 предназначен для защиты объекта, представляющего собой несколько пространственно разнесенных помещений или целое здание, от угроз, связанных с несанкционированной передачей информации подслушивающими устройствами или другими радиоэлектронными средствами. Комплекс позволяет осуществлять непрерывный радиоконтроль помещений объекта, а также проводить наблюдение за радиообстановкой вблизи объекта (например, регистрация радиообмена между мобильными приемо-передающими устройствами), анализ сигналов и выявление несанкционированных передач на поднесущих в одной или нескольких фазах сети электропитания, в проводных линиях и оптическом (инфракрасном) канале.

Комплекс имеет единый центр управления, в котором размещаются персональный компьютер, сканирующий приемник и микрокомпьютерный модуль RS1100/C. В качестве приемника используется сканер AR5000 фирмы AOR Ltd., который отличается расширенным динамическим диапазоном и повышенной помехозащищенностью.

Микрокомпьютерный модуль RS1100/C организует информационный обмен между персональным компьютером и микроконтроллером сканера, а также управляет периферийными устройствами.

Комплекс может быть укомплектован различными периферийными устройствами (внутрисистемная шина позволяет адресовать до 28 устройств, расположенных на расстоянии до 100 м от микрокомпьютерного модуля RS1100/C).

Для модернизации и расширения возможностей комплекса может использоваться широкая номенклатура периферийных устройств комплекса:

RS1000/K1 — дистанционно управляемый антенный переключатель для коммутации антенн и конвертеров;

RS1000/A — малогабаритная широкополосная камуфлированная антенна;

RS1000/L — конвертор для анализа сигналов в сети электропитания, проверки проводных и оптических линий;

RA1000/N — дистанционно управляемый генератор для нейтрализации подслушивающих устройств на частотах от 89 до 890 МГц;

RA1100/N — дистанционно управляемый генератор для нейтрализации подслушивающих устройств на частотах от 89 до 1600 МГц;

RS1100/Z — двухканальная удалённая акустическая система для идентификации радиомикрофонов методом акустического зондирования в контролируемых помещениях.

Прикладное программное обеспечение комплекса RS1100 представляет собой пакет 32-разрядных программ, работающих под управлением операционной системы Windows 95/98/NT. Программное обеспечение комплекса позволяет выполнять следующие базовые функции:

- проводить автоматическую адаптацию комплекса к окружающей электромагнитной обстановке;
- осуществлять управление комплексом радиоконтроля в автоматическом или ручном режиме;
- проводить автоматический поиск и обнаружение подслушивающих устройств;
- проводить анализ и исследование принимаемых радиосигналов, в том числе с использованием распределенной антенной системы;
- проводить автоматический контроль проводных коммуникаций;
- создавать и запускать на выполнение комплексные задания работы комплекса;
- осуществлять частотно-временной контроль и регистрацию работы радиоизлучающих устройств;
- производить дистанционное управление устройствами в автоматическом или ручном режиме.

Программно реализованы следующие инструментальные средства наблюдения:

- анализатор гармонического состава несущего колебания;

- цифровой анализатор спектра с запоминанием, накоплением и арифметическими операциями над спектрами;
- двухканальный цифровой осциллограф, отображающий сигналы с выходов демодулятора сканера (на базе звуковой платы компьютера) с регулируемой частотой дискретизации и возможностью записи реализаций на диск;
- корреляционный анализатор откликов акустического зондирования.

Управление процессами сканирования: последовательное сканирование заданных каналов в режиме SyberScan с обнаружением всех излучений в заданных диапазонах, детальный анализ обнаруженных сигналов и составление списка неизвестных излучений; параллельное сканирование в нормальном режиме, когда на каждой частоте настройки сканера антенный коммутатор с высокой скоростью переключает заданные каналы, а программа считывает уровни сигналов; параллельное сканирование заданных каналов с использованием аппаратуры модуля RS1100/C.

Идентификация сигналов подслушивающих устройств производится несколькими методами:

- появление нового излучения на фоне известных компьютеру, т. е. предварительно зарегистрированных в диаграмме загрузки радиодиапазона;
- идентификация методом анализа гармонического состава несущего колебания;
- идентификация методом акустического зондирования;
- идентификация методом корреляции сигналов опорной и текущей антенны.

Автоматизированный мобильный комплекс радиоконтроля RS предназначен для проведения радиомониторинга в заданном районе и может быть использован для задач радионаблюдения, радиоразведки и контроля каналов утечки информации. Перекрываемый диапазон частот от 9 кГц до 12 ГГц. В комплексе может использоваться система цифровой обработки сигналов (ЦОС) на базе процессора DSP56803 фирмы Motorola, позволяющая осуществлять векторный анализ сигналов на выходе ПЧ радиоприемного тракта. Программное обеспечение RS позволяет вести статистическую обработку сигналов за время предыдущего наблюдения, классифицировать сигналы и обнаруживать новые на фоне ранее накопленной усредненной панорамы. С использованием системы ЦОС программа позволяет наблюдать тонкую структуру сигнала с разрешением до 0,78 кГц. Многоканальный комплекс радиоконтроля зданий RS предназначен для защиты объекта, представляющего собой несколько пространственно разнесенных помещений или целое здание, от угроз, связанных с

несанкционированной передачей информации подслушивающими устройствами или другими радиоэлектронными средствами. Основным отличием нового комплекса является наличие в его составе анализатора, позволяющего проводить скоростной анализ спектра сигналов на выходе промежуточной частоты приемника в широкой полосе частот, например в полосе 8 МГц для приемника AR5000. При каждой перестройке приемника производится анализ радиообстановки в широкой полосе сразу по всем антеннам многоканальной системы. Комплекс проводит автоматизированное сравнение сигналов в контроллируемых помещениях и на внешней антенне. Из всех внутренних сигналов выбирается сигнал с максимальным уровнем и указывается его рейтинг (разница) относительно опорного сигнала на внешней антенне. Если вновь обнаруженный сигнал имеет положительный рейтинг, т. е. превышает уровень во внешней антенне, он заносится в графу «тревога» и может быть блокирован встроенным в систему генератором RS/N. Автоматическое блокирование может включаться и выключаться программно по желанию оператора. Таким образом, осуществляется принцип пространственной селекции, положенный в основу работы многоканальной системы. Комплекс контролирует до 25 каналов в радиодиапазоне и проводных линиях и допускает подключение удаленных устройств: конверторов, генераторов, акустических систем и т. д. Вся информация о сигналах помещается в компьютерную базу данных, которая в процессе эксплуатации системы заполняется автоматически без участия оператора. Имеется возможность визуального наблюдения в реальном времени одновременно до 7 каналов в широкой и узкой полосах.

RS digital M, RS digital Mobile M и RS digitalJet M предназначены для защиты объекта, представляющего собой несколько пространственно разнесенных помещений или целое здание, от угроз, связанных с несанкционированной передачей информации подслушивающими устройствами или другими радиоэлектронными средствами. Комплексы RS digital M и RS digital Mobile M отличаются лишь конструктивным исполнением. Комплекс полностью интегрируется в систему комплексной безопасности объекта и может управляться через компьютерную сеть. Это новая версия популярного комплекса RS turbo M с системой ЦОС и высокой скоростью работы. Имеется возможность визуального наблюдения в реальном времени одновременно до 8 каналов. Комплекс RS digital Mobile M изготовлен в ударопрочном кейсе Pelican. Комплекс RS digital M имеет стационарный вариант с расположением элементов в единой стойке. На базе контроллера RS digital M со встроенным 8-канальным коммутатором можно построить многоканальный комплекс требуемой конфигурации. Новая версия многоканального многофункционального комплекса радиоконтроля RS digital

Jet M построена на базе новых приемников RS Jet и может обеспечить непрерывный скоростной контроль эфира в больших офисах, зданиях, на отдельных территориях со скоростями анализа, близкими к скорости одноканального комплекса. Это позволяют достичь новые принципы построения распределенных систем и наличие мощных вычислителей.

Комплекс АРК-ДЗ-12 выполнен на базе аппаратуры АРК-Д1 (или АРК-ПК) и предназначен для автоматического обнаружения радиомикрофонов с числом помещений до 23 и определения их местоположения в каждом контролируемом помещении при управлении с центрального поста. В комплексе АРК-Д3 реализован ряд алгоритмов аппаратных средств, обеспечивающих наибольшее сокращение интервала обнаружения радиомикрофонов и автоматизации данного процесса.

Комплекс состоит из единого центра управления, в который входят:

- системный блок с комплексом АРК-Д1 или АРК-ПК (стационарный или в кейсе);
- антенные коммутаторы на 6 или 12 входов;
- управляющая стационарная ПЭВМ Р133 и выше;
- пакет СМО-ДЗ;
- НЧ блок для подключения управляющих целей;
- комплект кабелей;
- опорная антенна А5А с усилителем;
- устройство для контроля проводных сетей АРК-КПС (дополнительно);
- устройство для контроля ТВ-излучений (дополнительно),

а также оборудования для контролируемых помещений:

- широкополосной антенны АРК-2А;
- НЧ блока с дешифратором и усилителем;
- комплекта акустических колонок;
- микрофона;
- блока АРК СПМ формирования прицельных помех в диапазоне 65...1000 МГц (дополнительно).

Данный комплекс при минимальном участии оператора проводит анализ рабочего диапазона частот на наличие в контролируемых помещениях различных типов радиомикрофонов (в том числе и с простым скремблированием) и — по команде оператора — определение их координат.

В последнее время в связи с активным применением ЗУ с закрытием каналов излучения и использованием для этих целей различных частотных и амплитудно-частотных видов модуляции и манипуляций, возникла необходимость оперативного распознавания излучения таких ЗУ. С этой целью был разработан ряд аппаратно-программных

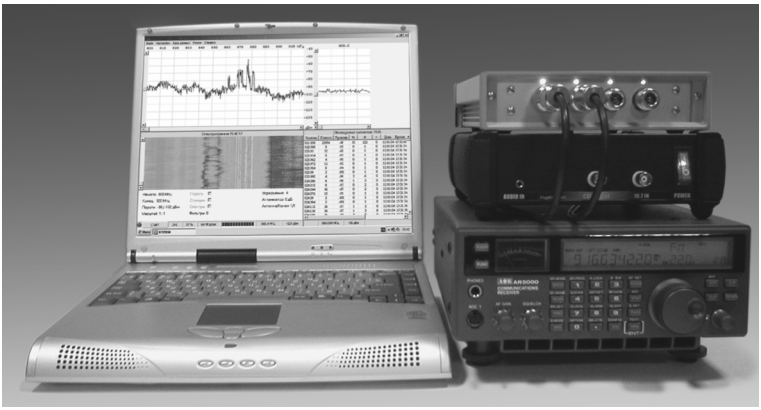


Рис. 2.38. Общий вид комплекса

комплексов, существенно отличающихся от своих предшественников. Принципы и особенности работы семейства этих комплексов рассмотрим на примере комплексов серии «Спектр».

Компьютерные комплексы серии «Спектр» (рис. 2.38) представлены стационарными и мобильными комплектами. Стационарный комплекс представляет собой мощную расширяемую аппаратную платформу, предназначенную для решения различных задач радиоконтроля и анализа электромагнитной обстановки, в том числе для автоматического обнаружения, идентификации, локализации и нейтрализации подслушивающих устройств, передающих данные по радиоканалу и проводным линиям. Комплекс может использоваться для организации как стационарных, так и мобильных постов радиоконтроля. Относительно высокая скорость обзора, чувствительность и разрешающая способность позволяют ему быстро и надежно выявлять и оценивать параметры любых источников сигналов и радиоизлучений в диапазоне частот от 0,6 кГц до 18 ГГц. В состав комплекса входят широкополосные антенны, антенный коммутатор, цифровой процессор радиосигналов и панорамный радиоприемник. Комплекс оснащается базовым программным обеспечением, предназначенным для автоматического обнаружения, анализа, классификации и регистрации сигналов. Комплекс может поставляться с дополнительными аппаратными и программными средствами, расширяющими возможности комплекса в различных условиях эксплуатации. Комплекс радиоконтроля использует несколько пространственно разнесенных антенн для выявления, оценки параметров идентификации источников радиоизлучений в контролируемых помещениях зданий, а также для организации постоянного контроля за радиообстановкой и поиска несанкционированных излучений на частотах от 40 до 3000 МГц. Программные средст-

ва пространственной классификации отбирают из всего множества обнаруженных сигналов только те, которые излучаются внутренними источниками, что значительно ускоряет и упрощает работу оператора при поиске каналов утечки информации. Система располагает векторным анализатором для исследования спектральных, временных и модуляционных характеристик радиосигналов в реальномвремени, а так же автоматическим регистратором для записи в память компьютера фонограмм демодулированных радиосигналов.

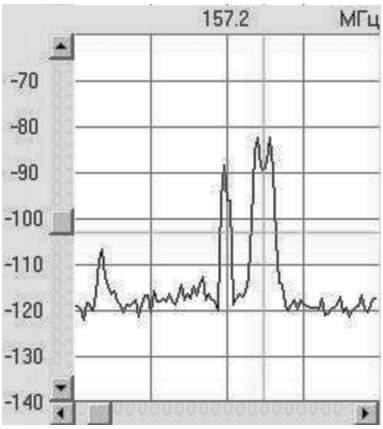


Рис. 2.39. Спектры сигналов станций персонального радиовызова

Скорость панорамного анализа (сканирования) в одноканальной конфигурации комплекса составляет от 90 до 100 МГц/с, а при работе с четырьмя антеннами снижается всего до 70...80 МГц/с. Относительно высокая производительность дает возможность комплексу обнаруживать и регистрировать спектры кратковременных передач и однократных сигналов (рис. 2.39). При полосе обзора 120 МГц комплекс достоверно выявляет сигналы с длительностью менее 1,5 с. Один цикл обзора частотного диапазона 40...3000 МГц занимает 25...30 с. При этом следует отметить, что технический параметр «скорость панорамного анализа» очень важен при оценке работоспособности аппаратуры радиоконтроля, так как в современных условиях широкое применение находят устройства негласного съема информации с промежуточным накоплением и дистанционным управлением. Излучения от данных изделий присутствуют в радиоэфире не постоянно, а некоторой периодичностью. В настоящее время комплекс не в полной мере соответствует современным требованиям по данному параметру. Хотя высокая чувствительность в сочетании с цифровым усреднением до 128 раз позволяет обнаруживать слабые сигналы с уровнями от -98 до -107 дБм (1 мкВ) без заметного снижения скорости обзора. Кроме того, цифровое усреднение значительно снижает вероятность реагирования комплекса на импульсные помехи. Обнаружение и различение сигналов выполняется цифровым параллельным анализатором спектра с разрешением 2 кГц (в режиме обнаружения). Погрешность оценки несущей частоты не более 2 кГц.

Высокое разрешение цифрового анализатора спектра позволяет различать узкополосные сигналы и выделять отдельные компоненты

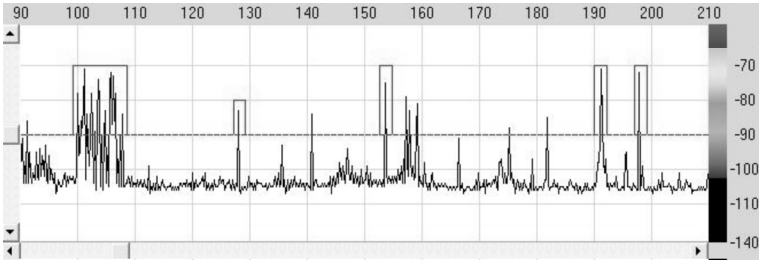


Рис. 2.40. Пороговые уровни

сигналов с дискретными спектрами. Спектры всех обнаруженных сигналов сохраняются в базе данных. Высокая разрешающая способность комплекса позволяет обнаруживать и правильно идентифицировать узкополосные сигналы устройств негласного съема информации несущие частоты, которых могут находиться рядом с центральными частотами «легальных источников». Для повышения достоверности пороговые уровни операций обнаружения и различения (рис. 2.40) могут задаваться в виде функций частоты с разрешением 200 кГц по частоте и 1 дБ по уровню. Подключение файла пороговых уровней позволяет исключить из обработки многочисленные легальные источники (телевидение, радиостанции, пейджинг, сотовая связь и т. д.), следовательно, снижает нагрузку на оператора.

Для различения и измерения параметров обнаруженных сигналов в комплексе используются методы статистического кластерного анализа. В процессе выполнения последовательных циклов обзора параметры обнаруженных сигналов подвергаются статистической обработке, что позволяет уточнять результаты процедур различения и свести к минимуму ошибки, связанные с нестационарностью спектров и изменением условий распространения радиоволн. Для каждого обнаруженного сигнала цифровой анализатор оценивает несущую частоту и ширину спектра с точностью до 2 кГц, абсолютное значение мощности на заданном антенном входе, фиксирует время/дату обнаружения и статистику появлений сигнала за все время наблюдений. Параметры обнаруженных сигналов сохраняются в базе данных и уточняются в процессе выполнения программой последовательных циклов сканирования.

Каждый однократно или многократно обнаруженный сигнал получает уникальный идентификатор и вместе со свойствами (центральная частота, ширина спектра, абсолютный уровень, регулярность обнаружения и т. д.) помещается в базу данных, которая в процессе эксплуатации системы создается и заполняется автоматически без участия оператора. Для повышения точности измерений в условиях

действия шума и для регистрации нестационарных сигналов используются различные режимы обработки реализаций спектров. Предусмотрена возможность усреднения от 2 до 128 реализаций, накопление максимальных и минимальных значений.

Дальнейшее развитие линейка программно-аппаратных комплексов «Спектр» получила в мобильных комплексах «Спектр-МК», «Спектр-Professional» и «Спектр-Экспресс».

Многоканальный комплекс радиоконтроля «Спектр-МК» предназначен для организации постоянного контроля за радиообстановкой и поиска несанкционированных излучений на частотах от 40 до 3000 МГц, а также обнаружения сигналов от устройств негласного съема информации с передачей данных по сети переменного тока с напряжением 220 В и слаботочным линиям. Комплекс использует несколько пространственно разнесенных антенн для выявления, оценки параметров и идентификации источников радиоизлучений на частотах 40...3000 МГц. Изделие «Спектр-МК» обеспечивает поиск устройств негласного съема информации с передачей сигналов по проводным линиям. С помощью конвертора проводных линий (КПЛ) возможно обнаружение и исследование низкочастотных сигналов, которые передаются по проводам сети переменного тока с напряжением 220 В и слаботочным линиям (пожарная и охранная сигнализации, телефонные линии) на несущих частотах в диапазоне от 600 Гц до 10 МГц.

Комплекс располагает векторным анализатором для изучения спектральных, временных и модуляционных характеристик радиосигналов в реальном времени, а также автоматическим регистратором для записи в память компьютера фонограмм демодулированных радиосигналов.

Аппаратура комплекса может питаться от сети переменного тока 220 В, бортовой сети автомобиля (+12 В) или встроенной аккумуляторной батареи. Это позволяет качественно решать задачи радиоконтроля, не привязываясь к конкретному источнику электроэнергии. Основные особенности комплекса: конструктивно встроенный конвертор проводных линий для поиска устройств негласного съема информации в силовых сетях, пожарной и охранной сигнализации, телефонных линия связи и т. п.; согласованные широкополосные приемные антенны АП-1МК на диапазон 300...3000 МГц с КСВ не более 1,8. Комплекс комплектуется высококачественными высокочастотными коаксиальными кабелями с погонным затуханием на частоте 3000 МГц не более 0,430 дБ/м; время автономной работы комплекса от встроенной аккумуляторной батареи не менее 6,5 ч, что позволяет обеспечить автономную работу, не привязываясь к конкретному источнику электроэнергии. Универсальная система энергообеспечения комплекса позволяет работать от бортовой сети автомобиля и

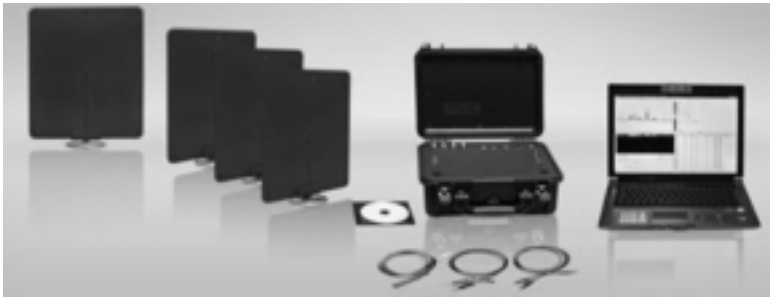


Рис. 2.41. Общий вид комплекса «Спектр-Professional»

заряжать встроенную аккумуляторную батарею. В состав комплекса входит конструктивно не связанная с ним управляющая ПЭВМ (ноутбук на базе энергосберегающей технологии Intel Centrino). Это позволяет помимо задач радиоконтроля решать и другие практические задачи, не привязываясь к аппаратуре радиоконтроля, кроме того, такое конструктивное решение позволяет оптимальным образом расположить ее на рабочем месте, исходя из условий освещенности и удобства работы. Специальная сумка- укладка для принадлежностей (кабель сетевой, кабель звуковой, кабель LPT, высокочастотные коаксиальные кабеля, широкополосные приемные антенны и т. д.), где каждая принадлежность или кабель находятся в своем обозначенном посадочном месте.

Комплекс «Спектр-Professional» (рис. 2.41). Идеи, заложенные в «Спектр-МК», получили свое дальнейшее развитие в комплексе «Спектр-Professional».

Многоканальный комплекс поиска устройств негласного съема информации «Спектр-Professional» предназначен для выявления излучений радиомикрофонов различных типов, радиостетоскопов, скрытых беспроводных видеокамер, а также обнаружения «опасных» сигналов от устройств негласного съема информации в сети 220 В, в слаботочных линиях (пожарная и охранная сигнализации, телефонные линии) и инфракрасном диапазоне. Комплекс использует несколько пространственно разнесенных антенн для поиска, оценки параметров и идентификации источников радиоизлучений на частотах 10...3000 МГц. С помощью СВЧ конвертора границы частотного диапазона расширяются до 18 ГГц. Встроенный автоматический конвертор проводных линий комплекса обеспечивает обнаружение «опасных» сигналов от сетевых микрофонов в различных проводных линиях, а подключение ИК датчика позволяет выявлять устройства негласного съема информации в инфракрасном диапазоне. Современное специализированное программное обеспечение комплекса позво-

Рис. 2.42. Пример изображения от беспроводной видеокамеры

ляет обнаруживать и идентифицировать сигналы от различных типов устройств негласного съема информации, в том числе использующих цифровые виды модуляции, шумоподобную структуру, режим псевдослучайной перестройки рабочей частоты и т. д.

С помощью встроенной системы видеозахвата (рис. 2.42) комплекс «Спектр-Professional» выводит на экран управляющего компьютера продетектированное изображение от скрытых беспроводных видеокамер. Обнаруженный опасный сигнал может быть записан на жесткий диск компьютера для последующего анализа.

Малые габаритные размеры, небольшая масса и удобство коммутации аппаратуры позволяют использовать многоканальный комплекс поиска устройств негласного съема информации «Спектр-Professional» в качестве мобильного поискового прибора. Аппаратура комплекса может питаться от сети 220 В, бортовой сети автомобиля (+12 В) или встроенной аккумуляторной батареи. Технические характеристики комплекса: частотный диапазон 10...3000 МГц; частотный диапазон СВЧ конвертора 3...18 ГГц; частотный диапазон КПЛ 0,0006...400 МГц; спектральный диапазон ИК датчика 320...1100 нм; скорость обзора более 1000 МГц/с; полоса обзора 0,1...5 МГц; разрешение анализатора спектра (режим анализа) 0,2 кГц; разрешение анализатора спектра (режим обнаружения) 2 кГц; чувствительность на антенном входе не хуже 2 мкВ; цифровые демодуляторы АМ, ЧМ, ФМ, векторный; время непрерывной работы от аккумуляторной батареи не менее 4,5 ч.

Дальнейшее развитие закладочных устройств привело к необходимости дальнейшей миниатюризации комплексов с сохранением их

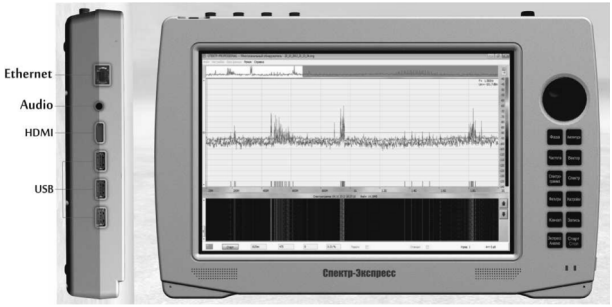


Рис. 2.43. Портативный комплекс «Спектр-Экспресс»

функциональных возможностей. Это реализовано в портативном комплексе поиска устройств негласного съема информации «Спектр-Экспресс» (рис. 2.43), предназначенном для выявления излучений радиомикрофонов различных типов, радиостетоскопов, скрытых беспроводных видеокамер, а также обнаружения сигналов от устройств негласного съема информации в сети 220 В, в слаботочных линиях (пожарная и охранная сигнализации, телефонные линии) и инфракрасном диапазоне. Комплекс позволяет решать «классические» задачи долговременного радионаблюдения заданных частотных диапазонов, а также задачи оперативного поиска «опасных» сигналов с возможностью их локализации в помещении или на местности.

Комплекс выполнен в виде моноблока. В портативный комплекс «Спектр-Экспресс» встроены: управляющая ПЭВМ, высокоскоростное радиоприемное устройство, аналого-цифровой преобразователь, четырехвходовый электронный антенный коммутатор, конвертор проводных линий, система видеозахвата и Li-Ion-аккумуляторная батарея. Комплекс оснащен встроенным сенсорным дисплеем с диагональю 12,1 дюйма. Комплекс использует до четырех пространственно разнесенных антенн для поиска, оценки параметров, идентификации и локализации источников радиоизлучений в частотных диапазонах 10...3000 МГц или 25...6000 МГц.

Автоматический конвертор проводных линий комплекса «Спектр-Экспресс» обеспечивает обнаружение сигналов от «сетевых» микрофонов в различных проводных линиях, а подключение ИК датчика позволяет выявлять устройства негласного съема информации, работающие в инфракрасном диапазоне. Скорость панорамного обзора в одноканальной конфигурации до 1150 МГц/с при разрешении по частоте 2 кГц. Высокая производительность дает возможность комплексу обнаруживать сигналы от радиомикрофонов, работающих в режиме накопления информации и кратковременной передачи её в эфир.

Обнаружение и различение сигналов выполняется цифровым па-

раллельным анализатором спектра с разрешением 2 кГц. Высокое разрешение цифрового анализатора спектра позволяет различать и обнаруживать узкополосные сигналы от радиомикрофонов, работающих рядом с легальными радиосредствами.

Специализированное программное обеспечение комплекса позволяет обнаруживать и идентифицировать сигналы от различных типов устройств негласного съема информации, в том числе использующих цифровые виды модуляции, шумоподобную структуру, режим псевдослучайной или программной перестройки рабочей частоты, сверхкоротких посылок (СКП) и т. д. Для обнаружения «опасных» сигналов в программном обеспечении реализован уникальный алгоритм разнесенного приема, имеющий три разновидности.

Абсолютно новый пользовательский интерфейс комплекса прост, интуитивно понятен и удобен. Управление аппаратурой возможно с помощью сенсорного экрана, с помощью внешней клавиатуры и манипулятора «мышь». Базовые настройки, контекстные меню с вспомогательными функциями, произвольное графическое масштабирование графиков и рабочих окон позволяют оператору максимально комфортно работать с комплексом.

Для удобства работы в комплексереализована возможность удаленного управления аппаратурой по локальной сети и Интернету.

С помощью встроенной системы видеозахвата комплекс выводит на сенсорный дисплей продетектированное изображение от скрытых беспроводных видеокамер. Обнаруженный сигнал можно записать в память компьютера для последующего анализа.

Компактные габаритные размеры, небольшая масса, удобство и оперативность коммутации аппаратуры позволяют использовать портативный комплекс «Спектр-Экспресс» в качестве одного из основных инструментов при проведении поисковых мероприятий. Основные тактико-технические характеристики комплекса: частотный диапазон 10...3000 (25...6000) МГц; частотный диапазон для проверки проводных линий 0,0006...10 МГц; спектральный диапазон ИК датчика 320...1100 нм; скорость панорамного обзора (при разрешении 2 кГц) до 1150 МГц/с; полоса обзора 0,1...50 МГц; разрешение (режим анализа) 0,2 кГц; разрешение (режим обнаружения) 2 кГц; чувствительность на антенном входе не хуже 2 мкВ; цифровые демодуляторы — NFM, WFM, векторный.

Высокоскоростной портативный аппаратно-программный комплекс радиоконтроля SpectrumJet (рис. 2.44) с встроенными антеннами предназначен для оперативного поиска несанкционированных передатчиков внутри помещений или на открытых площадках, зонах и т. д. Программное обеспечение специально написано под управление приемником через сенсорный экран. Например, для использования лупы

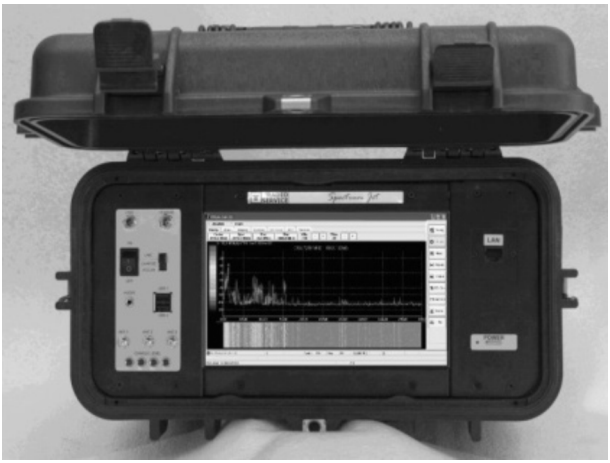


Рис. 2.44. Портативный аппаратно-программный комплекс SpectrumJet

при рассмотрении детального спектра сигнала достаточно провести пальцем по интересующему участку панорамы.

Основой новой версии поискового анализатора является радиоприемник RSJet, разработанный специально для решения задач радиомониторинга и поиска несанкционированных источников излучений. Применение этого радиоприемного устройства (РПУ) позволило увеличить скорость обзора при разрешении в 10 кГц до 5...10 ГГц/с, что позволяет обнаруживать и регистрировать для анализа сверхкороткие сигналы и сигналы с ППРЧ, а также исключительно эффективно производить накопление сигналов в широкой полосе частот, требующееся для реализации алгоритмов обнаружения сверхширокополосных сигналов. Встроенный цифровой приемник осуществляет решение всех основных задач мониторинга, фильтрации и демодуляции сигналов в случае, если таковая соответствует заданному стандартному типу.

Программное обеспечение позволяет вести статистическую обработку сигналов за время предыдущего наблюдения, классифицировать сигналы и обнаруживать новые на фоне ранее накопленной усредненной панорамы. Отметим, что все перечисленные операции осуществляются теперь гораздо быстрее, например процесс накопления и обработки данных для 1000 реализаций полосы в 19 ГГц занимает время всего около 40 минут. Конструктивно анализатор расположен в в вертикальном пластиковом кейсе с встроенными антеннами и 8,9" дисплеем. Опционально в состав анализатора может входить и комплект внешних антенн:

- широкополосная рамочная антенна RS/АБ для диапазона 30... 3000 МГц;

- направленная антенна на малогабаритном штативе RS/A/21 для диапазона 3...21 ГГц.
- активная магнитная антенна диапазона 9 кГц...30 МГц.

Также опционально анализатор может быть дополнен набором датчиков для анализа сигналов в сети электропитания, в проводных линиях и в оптическом диапазоне.

Управление анализатором осуществляется непосредственно с экрана (touch screen). Установленное программное обеспечение обеспечивает работоспособность анализатора не только в режиме анализа спектра, но и в режимах радиомониторинга и ручного управления. Программное обеспечение даёт возможность проводить анализ спектральных характеристик и соответствующие измерения, не прерывая процесс мониторинга. Для регистрации и демодуляции обнаруженного сигнала следует использовать ручной режим.

Рассматривая комплексы радиомониторинга нового поколения, необходимо отметить, что для поиска и локализации незаконно действующих источников излучений, использующих сложные алгоритмы маскировки во времени и по частотной шкале, необходимо использовать различные методы и алгоритмы поиска источников излучений: метод разнесенных антенн, метод разности панорам, эталонная панорама, метод сравнения с линией порога.

Применение данных методов вызывает необходимость использования различного программного обеспечения, состоящего, как правило, из нескольких программ. Современное специальное программное обеспечение представлено специальным программным обеспечением Inspector, рассмотренным ранее. Применение современных подходов к выявлению несанкционированных источников излучения реализовано в программно-аппаратных комплексах серии «Касандра».

«Кассандра» (рис. 2.45) — комплекс радиомониторинга нового поколения, предназначенный для поиска и локализации незаконно действующих источников излучений, использующих сложные алгоритмы маскировки во времени и по частотной шкале.

Комплекс радиомониторинга «Касандра-М» (рис. 2.46) представляет собой дальнейшее развитие комплексов семейства «Касандра».

В комплексе реализованы большинство известных на сегодняшний день методов и алгоритмов поиска источников излучений: метод разнесенных антенн, метод разности панорам, эталонная панорама, метод сравнения с линией порога. При решении задач радиомониторинга используются: оперативный или непрерывный радиомониторинг контролируемых помещений с сохранением всех результатов измерений и возможностью последующего их анализа; частотно-временной анализ для выявления демаскирующих признаков излуче-

Рис. 2.45. Комплекс радиомониторинга «Касандра»

Рис. 2.46. Комплекс радиомониторинга «Касандра-М»

ний, в том числе цифровых передатчиков, широкополосных сигналов и сигналов кратковременных передач; адаптивная линия порога, огибающая все легальные сигналы; специальные алгоритмы, уменьшающие вероятность ложной тревоги из-за флюктуации шумов и девиации сигналов; сохранение всех результатов радиомониторинга для объективного контроля и периодического контроля изменения радиоэлектронной обстановки в контролируемых точках; полноценное управление комплексом по компьютерной сети, в том числе и передача демодулированного аудиосигнала в реальном масштабе времени. Основные технические характеристики комплекса: диапазон рабочих частот 25...3000 МГц; скорость обзора типовая 120...140 МГц/с при полосе пропускания 16 кГц; чувствительность по входу не хуже 2 мкВ при полосе 1 кГц и отношении с/ш 6 дБ; питание сеть 220 В или автономное питание.

Комплекс радиомониторинга (комплекс радиоконтроля) «Кассандра М» предназначен для поиска и локализации незаконно действующих передатчиков, использующих различные, в том числе сложные, алгоритмы маскировки. Позволяет вести непрерывное круглосуточное наблюдение за радиоэфиром в полосе частот комплекса. Пользователь вместе с сочетанием уникального программного обеспечения и самых передовых аппаратных средств получает возможность полноценного отложенного анализа и ведения радиоконтроля по сети.

Область применения охватывает проведение спецобследование объектов, помещений, борьбу с промышленным шпионажем, поиск нелегально установленных радиопередатчиков, организация стацио-

Рис. 2.47. Комплекс радиомониторинга и анализа сигналов «Кассандра-СО»

нарных и мобильных постов радиоконтроля. Программное обеспечение комплекса отличается современной концепцией построения, «дружелюбием» по отношению к оператору, в нём учтено всё, что может понадобиться при оценке защищенности радиоспектра от утечки информации. Компактность и малый вес. Высокая скорость сканирования, широкий динамический диапазон, «чистота» от внутренних и интермодуляционных помех. Возможность наращивания функций, в частности опционный программный модуль DTest позволяет производить анализ топологии сетей DECT, GSM, Bluetooth, проверять сигналы на принадлежность к стандарту DECT, TETRA, GSM, Bluetooth, APCO25, демодулировать APCO25, отображать PalTV, NTSC, векторную диаграмму сигналов.

Комплекс радиомониторинга и анализа сигналов «Кассандра-СО» (рис. 2.47) предназначен для постоянного или периодического контроля радиообстановки, выявления и анализа несанкционированных радиоизлучений. Может служить для проведения спецобследований.

Аппаратным ядром комплекса является современный двух канальный приемник нового поколения. В комплексе реализован удобный пользовательский интерфейс, многозадачность, применяется адаптивный порог. Управление по LAN с возможностью удалённого управления через каналы передачи данных (Интернет и др.). Универсальный анализ спектров и документирование. Возможность проведения полноценного отложенного анализа. Настраиваемая математическая обработка полученных данных. Синхронный и асинхронный режим работы. Возможность анализа цифровых сигналов DECT, TETRA, GSM, APCO-P25, BlueTooth, Wi-Fi. Запись IQ. Диапазон рабочих частот от 9 кГц до 21 ГГц. Чувствительность двухканального РПУ по входам: в диапазоне от 30 до 3 000 МГц не менее -170 дБ·Вт/Гц; в диапазоне от 3 до 18 ГГц не менее -150 дБ·Вт/Гц. Динамический диапазон каждого канала РПУ по одному сигналу в диапазоне частот

Рис. 2.48. Общий вид комплекса «Эврика»

от 30 до 3000 МГц в режиме обнаружения не менее 90 дБ. Скорость обзора: в диапазоне от 30 до 3000 МГц 2000 МГц/с; в диапазоне от 3 до 18 ГГц 1000 МГц/с. Автономная работа не менее 2 часов.

Комплекс «Эврика» (рис. 2.48) предназначен для автоматизированного и ручного выявления аналоговых и цифровых радиопередатчиков. Комплекс может эксплуатироваться в мобильном или стационарном вариантах (распределенная система радиоконтроля). Поиск сигналов и обработка информации максимально автоматизированы, имеется возможность исследования и анализа сигналов в ручном режиме. Комплекс позволяет накапливать и применять опыт, полученный в процессе работы, создавая собственные правила поиска и критерии отбора сигналов. Имеется возможность обмениваться этими правилами и критериями с другими пользователями. Пользователь может сам индивидуально конфигурировать программную оболочку исходя из специфики решаемых задач и оперативной обстановки.

Аппаратным ядром комплекса является цифровой панорамный приемник нового поколения Р300 на базе I/Q-технологии обработки сигналов, реализующий высокопроизводительные решения для приема и обработки сигналов, включая распределенные сетевые архитектуры.

Диапазон рабочих частот приемника (30...3600 МГц) перекрывает наиболее распространенные полосы частот радиопередатчиков. Диапазон сканирования может быть расширен до 30 кГц (в КВ и ДВ диапазоны) и до 12,3 ГГц (в СВЧ диапазон). Модуль приема КВ и ДВ диапазонов является полноценным КВ приемником. СВЧ конвертер представляет собой понижающий преобразователь частоты с высокой чувствительностью и подавлением побочных каналов приема на 40 дБ.

Цифровой панорамный приемник Р300 разработан специально для построения современных комплексов радиоконтроля. Технические характеристики Р300 позволяют эффективно обнаруживать большинство известных радиосигналов, обрабатывать информацию в цифровом виде и в реальном времени предоставлять ее пользовате-

лю для анализа и принятия решения. P300 реализован по технологии инфрадинного приемника с нулевой промежуточной частотой. Для работы в условиях загрузки спектра сигналами мощных передатчиков (вблизи базовых станций, ретрансляторов и т. д.) P300 оснащен встроенными преселекторами, которые минимизируют воздействие на приемный тракт внеполосных сигналов.

Аналого-цифровое преобразование сигнала выполняется P300 параллельно по синфазному и квадратурному каналам промежуточной частоты с помощью высокоскоростных АЦП. Модуль цифровой обработки сигналов, к задачам которого относятся квадратурное гетеродинирование, фильтрация и демодуляция, выполнен на базе высокопроизводительной ПЛИС и обеспечивает параллельную обработку сигналов в реальном времени. При этом набор цифровых фильтров с полосой от 1 кГц до 56 МГц позволяет обрабатывать сигналы с наиболее оптимальным соотношением сигнал/шум.

P300 имеет встроенный 4-канальный антенный коммутатор, который позволяет реализовать алгоритмы разнесенного приема сигналов без использования дополнительного оборудования. Время переключения каналов коммутатора 1 мкс. Кроме стандартного интерфейса USB 2.0, P300 оснащается высокоскоростным интерфейсом 802.3 (Ethernet) и собственным буфером данных. Это позволяет не только значительно повысить скорость сканирования, но и использовать приемник в качестве удаленной рабочей станции в локальной сети или Интернете с возможностью дистанционного управления всеми функциями приемника, а также диагностики состояния его внутренних модулей (модуля питания, цифровой обработки, ВЧ тракта).

Интеллектуальная система управления питанием P300 позволяет использовать любой доступный вид электропитания — сеть 110–220 В, бортовое питание или питание от встроенного аккумулятора. При питании от аккумулятора можно полностью автономно использовать не только сам приемник, но и подключаемую к нему периферию.

P300 поставляется в OEM версии, которая является универсальной платформой для построения комплексов радиоконтроля и радиомониторинга. Разработчиками предлагаются наборы библиотек, реализующие программный доступ ко всем функциям аппаратной части P300, и открытые исходные коды для управления всеми функциями приемника.

Програмное обеспечение комплекса позволяет производить высокоскоростной панорамный анализ радиочастотного спектра одновременно в частотной и временной областях. Это позволяет оператору визуально отследить хронологию появления сигналов на участке спектра и их частотно-временные характеристики. Любой участок

сканируемого спектра может быть расширен для детального анализа структуры сигналов.

Панорамы строятся последовательно-параллельным методом. Спектр последовательно «склеивается» из участков анализируемых приемником в параллельном режиме.

Комплекс позволяет устанавливать полосу параллельного анализа от 4 до 58 МГц. Сужение полосы анализа приводит к повышению разрешающей способности анализатора, но уменьшает скорость сканирования, т. е. оператор сам может выбрать разрешение, наиболее оптимальное для его задачи спектрального анализа. Для различения сигнала от шума в комплексе «Эврика» предусмотрены два вида амплитудного порога: автоматический, когда решение сигнал/шум принимается программой оболочкой, и ручной, когда пользователь задает минимальный уровень сигнала. При этом ручной порог может задаваться в виде ломанной линии по поддиапазонам. Для режима «водопад» предусмотрена возможность задания отдельного порога. Для каждого обнаруженного сигнала программная оболочка позволяет оценить несущую частоту, ширину спектра, амплитуду, фиксирует дату/время обнаружения и статистику появления сигнала за все время наблюдений. Параметры каждого обнаруженного сигнала автоматически сохраняются в списке сигналов, который является частью базы данных комплекса.

В списке сигналов оператору доступны поля, в которые он может вносить информацию вручную. Оператор может указать вид модуляции, тип сигнала, уровень опасности сигнала или оставить текстовые примечания в соответствующих полях.

При повторном обнаружении ранее сохраненные параметры сигнала уточняются, что позволяет свести к минимуму ошибки, связанные с нестационарностью спектров сигналов и изменением условий распространения радиоволн. Параметры сигналов уточняются при работе алгоритмов автоматического распознавания модуляций. Программа комплекса автоматически вычисляет и включает в базу данных статистические характеристики параметров сигналов. Так, например, вычисляются процент появления сигнала и пик-фактор, позволяющий оценить периодичность появления сигнала в эфире на протяжении всего времени наблюдения. Использование статистических характеристик позволяет отсеивать случайные помехи и автоматизировать процесс выявления несанкционированных передатчиков с накоплением информации. В режиме панорамного анализа комплекс имеет уникальный инструмент, позволяющий визуализировать статистику появления сигналов на определенных участках спектра. Этот инструмент вместе с анализом статистических характеристик сигнала

позволяет автоматизировать процесс обнаружения сигналов с псевдослучайной перестройкой частоты (ППРЧ).

Программная оболочка хранит всю информацию в реляционной базе данных, когда поля одних списков связаны с полями других списков. Во взаимосвязанных списках вместе с параметрами обнаруженных сигналов хранятся относящиеся к ним фонограммы, спектральные реализации и изображения мгновенных спектров сигналов (медиаданные). Пользователь может легко просмотреть все фонограммы, которые записывались на определенной частоте, выбранной в списке сигналов, просто выбрав эту частоту в списке сигналов и перейдя в список медиаданных. Кроме того имеется возможность экспортировать списки в файл в формате cvs. Данный формат файла поддерживается большинством табличных редакторов, таких как например MSExcel и OpenOfficeCalc.

Программа поддерживает двухэкранный режим рабочего стола, который позволяет максимально эргономично организовать рабочее пространство оператора и оптимизировать расположение окон с графической информацией и списков как в режиме анализа сигналов, так и при работе с базой данных. Возможности комплекса могут легко наращиваться за счет модернизации программной оболочки: от базовой до экспертной версии и от локальной до сетевой конфигурации.

Наличие анализатора спектра позволяет исследовать частотную структуру сигнала, девиацию поднесущих частот и т. д. Для сигналов со специфическим видом спектра данный режим дает возможность оператору провести также визуальную идентификацию сигналов.

Программная оболочка комплекса позволяет проводить детальный спектральный анализ обнаруженных сигналов в полосе от 1 кГц до 56 МГц с разрешением по частоте до 1 Гц (в полосе 1 кГц) и до 4 кГц (в полосе 56 МГц). В режиме сканирования спектральные реализации сигналов перед отображением усредняются с заданной кратностью. Для уменьшения влияния динамического шума в анализаторе спектра, а также для обнаружения кратковременных сигналов используется специальная функция — настраиваемое время измерения, при этом регистрация спектров нестационарных и однократных сигналов возможна в режиме накопления максимальных частотных составляющих.

Векторный анализатор позволяет отображать принятый радиосигнал на комплексной плоскости и выводит на экран диаграмму изменения комплексной огибающей принимаемого сигнала во времени. Анализ траектории вектора комплексной огибающей сигнала позволяет распознать как аналоговые виды модуляции (AM, FM), так и цифровые сигналы с многопозиционной фазовой или амплитудно-фазовой манипуляцией (PSK, BPSK, QPSK, ASK и QAM), использу-

емые в стандартах GSM и CDMA. В зависимости от передаваемого символа значения фазы и амплитуды таких сигналов попадают на определённые точки комплексной плоскости. Векторный анализатор в настоящее время является наиболее перспективным инструментом визуализации и технического анализа сигналов. Векторная диаграмма может быть представлена либо в виде линий, соединяющих точки на плоскости, либо в виде самих точек. Оператор может сам выбрать удобное для него представление.

Изменение спектров радиосигналов во времени отображается на мониторе в виде «водопада» и представляет собой цветовую проекцию амплитуды сигнала на частотно-временную плоскость. Применение режима «водопад» позволяет сохранить частотные панорамы, полученные за все время наблюдения. При этом применение статистических методов анализа изменения электромагнитной обстановки помогает обнаружить и идентифицировать сигналы от устройств негласного контроля информации с ППРЧ, передатчиков с накоплением, передатчиков с дистанционным управлением и активацией голосом (VOX).

Режим осциллографа позволяет отобразить структуру сигнала во временной области по I- и Q-каналам в двух параллельных окнах. Это дает возможность эффективно идентифицировать сходные виды модуляций, различение которых другими методами затруднительно, например частотную и фазовую манипуляции (FSK, PSK). Кроме специфических функций, которые дает параллельный анализ I- и Q-каналов, осциллограф может использоваться и для обычного анализа сигналов во временной области.

Программа комплекса позволяет реализовать три вида автоматических маркеров, определяющих минимальное и максимальное значения сигнала, а также уровень шума и пять видов ручных маркеров (односигнальные и дифференциальные). Для облегчения частотной подстройки реализована функция автоматического совмещения маркера и частоты настройки приемника. Данная функция особенно необходима для устранения набега фазы комплексной огибающей сигнала в режиме векторного анализатора.

Для анализа низкочастотной составляющей сигнала в комплексе предусмотрены режимы анализатора спектра и осциллографа для демодулированного сигнала. Эти режимы, в частности, позволяют обнаружить в демодулированном сигнале импульсные посылки (DTMF-коды) или исследовать спектральные характеристики демодулированного сигнала в частотной и временной областях.

Сетевой интерфейс позволяет объединять несколько постов в единую сеть радиомониторинга объекта. Комплекс может быть сконфигурирован для работы с приемником Р300 в следующих режимах:

ведущего приемника-источника данных о параметрах сигналов при сканировании радиоэфира; ведомого приемника-источника данных при исследовании сигналов, например при демодуляции без прерывания сканирования; удаленного коммутатора для применения алгоритма разнесенного приема сигналов в многозонной конфигурации при значительном удалении контролируемых помещений.

Эксперименты показали, что использование коммутаторов с числом каналов более 4-х крайне неэффективно для метода разнесенного приема, что связано с большими потерями в антенно-фидерном тракте при контроле удаленных помещений. Именно поэтому для мониторинга большого количества помещений целесообразно использовать удаленные приемные модули Р300 со встроенными 4-канальными антенными коммутаторами. Для передачи данных между приемниками используется штатная локальная компьютерная сеть объекта. В такой конфигурации приемные устройства с 4-мя зонами контроля каждое и пункт контроля могут располагаться на произвольном удалении друг от друга в пределах одной локальной сети передачи данных. Комплекс поддерживает подключение до 8 приемников Р300 в режиме удаленного коммутатора, что позволяет анализировать до 32 УКВ каналов, а также неограниченное количество приемников в режиме ведомого для исследования сигналов без прерывания режима сканирования. Аппаратная часть комплекса позволяет подключать дополнительные приемники, как через ПЭВМ, так и напрямую в сеть Ethernet в режиме сетевого устройства.

В ручном или автоматическом режиме для каждого сигнала в базе данных могут быть записаны и сохранены фонограммы: демодулированного сигнала; комплексные данные; мгновенный спектр в виде изображений.

Модуль работы со звуковыми файлами АПК предоставляет оператору широкий инструментарий для редактирования и анализа записанных фонограмм, в том числе удаление фрагментов для очистки фонограммы от помехи пауз; регулировка АЧХ фильтров эквалайзера для повышения разборчивости речи; автоматическая регулировка усиления для воспроизведения слабых сигналов; воспроизведение фонограмм с различной скоростью; инвертирование спектра записанного сигнала в заданной полосе для распознавания передатчиков и микрофонов с некоторыми типами маскираторов речи.

Массивы комплексных данных позволяют полностью восстановить записанный сигнал сразу во всех представлениях — спектральном, «водопаде», осциллографе, I- и Q-каналов и векторном анализаторе. Реализации могут быть воспроизведены оператором в пошаговом режиме, что позволяет анализировать переходные процессы и

производить идентификацию передатчика по характеру роста и спада огибающей сигнала в момент включения и выключения передатчика.

Использование в алгоритме программы разнесенного приема для обнаружения передатчиков в ближней зоне по разности абсолютных уровней сигналов на удаленных антеннах не позволяет с высокой достоверностью определить внутренний источник сигнала. Это связано с рядом особенностей распространения радиоволн как в условиях городской застройки, так и внутри помещений. Поэтому в комплексе применен статистический метод оценки расположения передатчика в ближней зоне, который основан на выводах из анализа данных разнесенного приема и большой экспериментальной базы. Это позволяет с высокой достоверностью выявлять «внутренние» источники в условиях города.

Режим параметрической корреляции предназначен для автоматизированного выявления передатчиков, использующих механизм акустопуска (VOX). Создание «подзвучки» в проверяемом помещении позволяет выявить сигналы, которые отсутствуют до и после «подзвучки». Одной клавишей можно запустить режим автоматического выявления новых сигналов относительно заданного момента времени, например с момента начала совещания в защищаемом помещении. В комплексе реализованы собственные алгоритмы автоматического распознавания большинства наиболее распространенных видов модуляций сигналов. Эти алгоритмы позволяют при достаточном соотношении сигнал/шум в полностью автоматическом режиме распознать виды модуляции сигналов, которые наиболее часто используются в несанкционированных передатчиках или устройствах управления ими: AM, FM, PM, ASK, FSK, PSK, QPSK, BPSK.

При распознавании вида модуляции комплекс автоматически уточняет основные параметры сигнала, такие как центральная частота и полосасигнала, и актуализирует соответствующие ячейки списка сигналов.

База знаний является уникальным инструментом комплекса, в котором использованы возможности экспертных систем для автоматизированной обработки информации и принятия решения. База знаний содержит инструменты автоматической классификации сигналов в базе данных: программируемые фильтры, которые позволяют автоматизировать распределение сигналов по группам; планировщик заданий для программирования работы комплекса в автоматическом режиме; база данных эталонных реализаций, которые могут быть использованы для визуальной идентификации видов модуляции и типа сигнала.

База знаний позволяет оператору централизовано и непосредственно в оболочке комплекса систематизировать все опытные данные

за все время работы с комплексом на различных объектах. Комбинации программируемых фильтров и заданий планировщика позволяют пользователю создавать макросы и настраивать оболочку комплекса под собственные задачи самостоятельно без привлечения разработчиков программного обеспечения, используя исключительно дружественный пользовательский интерфейс комплекса. Возможности экспорта и импорта элементов базы знаний открывают широкие возможности для обмена опытом между пользователями комплекса.

Программные фильтры — это инструмент автоматической сортировки списка сигналов по заданным параметрам. Фильтры позволяют скрывать ненужные сигналы и выделять группы сигналов по заданным признакам. Фильтры объединяются в наборы, количество которых не ограничено. Наборы применяются к базе данных как матрицы для выделения сигналов определенного типа. Наборы фильтров могут экспортироваться и импортироваться для обмена опытом между пользователями. При этом использование групп признаков, а не фиксированной сетки частот позволяет одинаково эффективно применять накопленную информацию о признаках «опасных» и легальных сигналов в регионах сразличными частотными назначениями.

Инструменты программирования работы комплекса в автоматическом режиме планировщика позволяют использовать комплекс для контроля эфира полностью автономно, например во внерабочее время. При появлении сигнала с любым из определенных заранее признаком комплекс полностью автоматически производит заданный набор действий (выполняет задание). Задания могут состоять из неограниченного количества действий, таких как: запись реализации для последующего анализа, или фонограммы демодулированного сигнала; запуск алгоритмов распознавания модуляции; изменение атрибута сигнала; запуск внешней программы.

Третьим элементом базы знаний являются эталоны. База данных содержит ранее записанные эталонные реализации сигналов в виде фонограмм, изображений или комплексных данных, которые можно восстановить в любом из видов представлений. Оператор может сравнить в параллельном окне любой сигнал, принятый из эфира, с имеющимся в банке эталонов образом, причем в любой из доступных в комплексе реализаций.

В качестве эталона может использоваться ранее записанная фонограмма сигнала. В списке эталонов удобно систематизировать накопившиеся у оператора знания о внешнем виде тех или иных сигналов, как «опасных», так и легальных. «Эврика» позволяет сохранять эталонную панораму — усредненный частотный спектр во всем диапазоне частот и выводить ее одновременно с текущей панорамой в

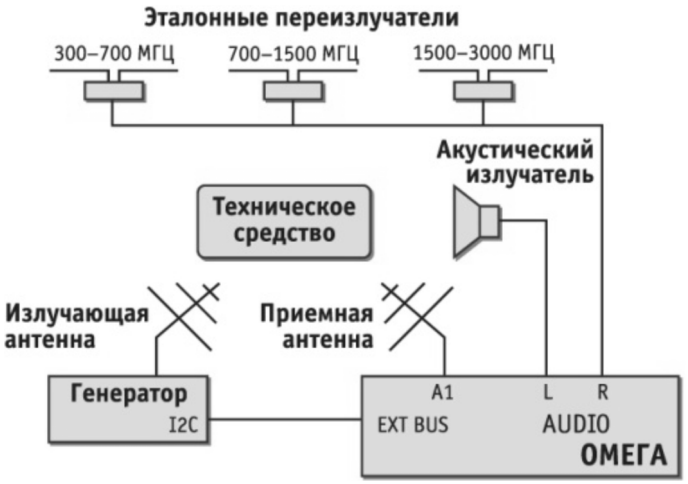


Рис. 2.49. Принципиальная схема работы комплекса

режиме сканирования для визуальной оценки изменения электромагнитной обстановки на объекте в дифференциальном режиме.

Высокочастотное навязывание. Активное использование метода высокочастотного навязывания, реализуемого с помощью как специализированных средств несанкционированного получения информации, так и технических средств, находящихся в облучаемых помещениях, требует применения новых подходов, один из которых связан с созданием в контролируемых помещениях тестового высокочастотного навязывания. Задача обнаружения технических устройств и объектов, обладающих свойствами эндовибрации, основывается на ВЧ воздействии на обследуемые объекты, поиска возможных переизлучений от них и анализа переизлученного сигнала на наличие акустической модуляции. При этом необходимо одновременно воздействовать на объект акустическим сигналом.

С целью выполнения задачи по обнаружению и локализации объектов, обладающих свойствами эндовибрации, были разработаны аппаратно-программные комплексы для исследования модуляции переизлученных колебаний (рис. 2.49). Комплексы представляют собой комплект оборудования, предназначенный для обнаружения резонансных переизлучателей (эндовибраторов и других вторичных излучателей). Они могут размещаться в технических средствах обработки информации, средствах оргтехники, помещениях, предметах интерьера и т. п. Принцип работы комплекса основан на облучении обследуемых объектов высокочастотным электромагнитным полем (от 100 до 3000 МГц) при одновременном акустическом воздействии с последующим приемом переизлученного (отраженного) сигнала и его

анализом на наличие модуляции, обусловленной этим акустическим воздействием. При этом во всем рабочем диапазоне обеспечивается заданная чувствительность и максимальное значение подводимой к антенне мощности облучаемого сигнала.

Аппаратура выявления резонансных переизлучателей состоит из направленных широкополосных приемной и передающей антенн (например, спиральных), расположенных в одной плоскости (пространственное разделение зондирующего и отраженного сигналов) и направленных на предмет обследования. Облучающий сигнал в передающей антенне формируется перестраиваемым ВЧ генератором. С выхода приёмной антенны отраженный сигнал поступает на приемник с панорамным анализатором спектра. Частота настройки приемника перестраивается синхронно с перестройкой частоты ВЧ генератора во всем рабочем диапазоне частот.

Резонансная частота переизлучателя определяется его конструктивными особенностями. Наиболее вероятно ожидать наличия эндовибраторных свойств у обследуемых предметов в диапазоне частот от 0,1 до 1,8 ГГц, так как в этом диапазоне при хорошей отражающей способности металлических предметов со сравнительно небольшими геометрическими размерами достаточно высока проникающая способность электромагнитных волн в строительных конструкциях. Акустический излучатель обеспечивает создание на обследуемой поверхности необходимого звукового, давления. Акустический сигнал с частотой F_a формируется НЧ генератором.

Поиск эндовибраторов производится по обнаружению тональной (частотой F_i) модуляции при настройке аппаратуры на резонансную частоту эндовибратора.

Наличие модуляции отраженного радиосигнала сигналом с частотой акустического воздействия определяется по прослушиванию ее на выходе приемника (в режиме амплитудной модуляции) или с помощью панорамного анализатора спектра.

Сигналы-отклики аппаратуре высокочастотного облучения могут давать микрофонирующие пустотелые металлические предметы, а также протяженные тонкостенные металлические изделия. Отличием сигнала-отклика от резонансного эндовибратора является его наличие в узкой полосе.

Для сигналов, отраженных от пассивных вторичных излучателей, характерна амплитудная модуляция за счет изменения под действием акустического давления эффективной площади рассеяния. Для других видов модуляции необходимы нелинейные преобразования воздействующего сигнала, которые должны быть реализованы на активных радиоэлектронных компонентах.

Следует учитывать, что при наличии микрофонирующих предметов имеется возможность использовать их для организации канала снятия речевой информации из помещения. На эффективность работы аппаратуры существенное влияние могут оказывать внешние электромагнитные поля. Поэтому поиск эндовибраторов целесообразно проводить в наиболее благоприятное с точки зрения отсутствия помех время. Перед проведением обследования строительных конструкций следует убрать из зоны облучения экранирующие предметы: металлические шкафы, сейфы, зеркала и т. д.

Размеры обследуемой зоны определяются расстоянием от нее до антенны аппаратуры облучения и шириной ее диаграммы направленности. При обследовании акустический излучатель необходимо располагать за аппаратурой облучения (для исключения приема модулированных ВЧ сигналов отраженных от этого излучателя). Кроме выявления специально внедренных эндовибраторов или элементов конструкций, обладающих эндовибраторными свойствами, следует учитывать возможность снятия информации, обрабатываемой установленными в помещениях техническими средствами: телефонными аппаратами, пультами прямой связи, аппаратурой системы звукоусиления и т. д. Эти технические средства могут иметь в своем составе резонансные переизлучатели, образованные элементами конструкций и электрических схем, а также нелинейные элементы, параметры которых изменяются при протекании через них электрических сигналов. В ряде случаев, особенно при отсутствии экранирования, с помощью аппаратуры высокочастотного облучения можно прослушать речевую информацию, обрабатываемую данными техническими средствами. Модулированный ВЧ сигнал может быть принят как от облучаемого предмета, обладающего эндовибраторными свойствами, так и от постороннего источника излучения (сигналы радиовещательных станций, излучения технических средств и т. п.).

По следующим признакам можно судить о том, что облучаемый объект обладает эндовибраторными свойствами:

- отклик появляется при направлении антенной системы на облучаемый объект;
- в наушниках прослушивается акустический фон помещения (при выключении озвучивающего сигнала отклик пропадает);
- легкое постукивание диэлектрическим предметом по облучаемому предмету прослушивается в наушниках аппаратуры;
- конструктивные особенности технических средств или предметов интерьера (отсутствие экранирования; наличие высокочастотных резонансных контуров или резонансных антенн; наличие подвижных элементов конструкции, перемещающихся под дейст-

вием акустических или вибрационных сигналов; наличие акустических излучателей и др.);

- возможные неисправности схем защиты (обрыв экранирующего соединения) или нарушение правил эксплуатации технических средств (отсутствие заземления), слабое крепление электропроводящих элементов конструкции (незакрепленные металлические корпуса технических средств, элементы коробов вентиляции, осветительного оборудования и т. п.);
- внедренные в ограждающие конструкции помещения, устновленные в них предметы интерьера или технические средства специальные средства съема информации.

На основе проведенного анализа принимается решение о необходимости устранения выявленных недостатков, удаления из помещения модулирующих отражателей или о проведении дополнительной экспертизы.

Автоматизированный комплекс выявления акустопараметрических каналов «Крона-А1» (рис. 2.50) предназначен для обнаружения и локализации электронных устройств негласного получения информации (ЭУНПИ), передающих данные по радиоканалу, использующих все известные средства маскирования, выявления каналов утечки информации, созданных за счет акустопараметрических преобразований, а также для решения широкого круга задач радиомониторинга. Позволяет обнаруживать пассивные и полуактивные акустопараметрические электромагнитные отражатели (эндовибраторы) в диапазоне частот от 30 МГц до 12 ГГц. Комплекс реализует в себе наиболее передовые алгоритмы обнаружения ЭУНПИ. Применение нескольких алгоритмов обнаружения, каждый из которых основан на индивидуальных прин-

Рис. 2.50. Комплекс выявления акустопараметрических каналов «Крона-А1»

ципах демаскирования ЭУНПИ, позволяет с высокой степенью достоверности определить наличие ЭУНПИ, имеющих средства маскировки как по алгоритмам модуляции, так и по способам передачи (ЭУНПИ с цифровыми каналами передачи данных, с накоплением информации, с перестраиваемой частотой и т. д.).

«Крона-А1» может использоваться как для экспресс-анализа наличия радиопередающих электронных устройств для несанкционированной передачи информации (ЭУНПИ) в контролируемом помещении, так и для долговременного круглосуточного мониторинга электромагнитной обстановки в одном или нескольких контролируемых помещениях. Комплекс использует эффективный алгоритм выделения полезного информативного сигнала в сложной помеховой обстановке. Это позволяет получить достоверные результаты поиска каналов утечки речевой информации, образованных за счет акустопараметрических преобразований. Комплекс позволяет решать следующие задачи: обнаружение и локализация ЭУНПИ, использующих все известные средства маскирования; обнаружение пассивных и полуактивных акустопараметрических электромагнитных отражателей (эндовибраторов); автоматическое распознавание цифровых каналов передачи данных; анализ сигналов в силовых сетях и слаботочных линиях в диапазоне частот до 400 МГц, исследование ИК излучений; контроль диапазона частот, фиксированных частот, сетки частот; выполнение комплексных заданий; анализ сигналов с нескольких антенн, используя встроенный антенный коммутатор.

Кроме унифицированных комплексов, разработаны комплексы, специально предназначенные для выявления пассивных и полуактивных акустопараметрических электромагнитных отражателей (эндовибраторов).

Широкополосный регистратор модуляции вторичного излучения «Ревиз-5000» (рис. 5.51) предназначен для исследования отражающих свойств радиотехнических объектов в диапазоне частот 30... ...5000 МГц, а также для исследования высокочастотных кабелей методом ВЧ навязывания.

Принцип действия комплекса основан на облучении объекта обнаружения электромагнитными и акустическими колебаниями с последующим приемом и анализом отраженного колебания на наличие модуляции акустическим сигналом. Функциональная схема комплекса «Ревиз-5000» приведена на рис. 2.52. Комплекс состоит из управляющей ПЭВМ, блока сопряжения, перестраиваемого генератора высокой частоты, усилителя мощности, приемника, направленного ответвителя, приемо-передающей антенны (или приемной и передающей антенн), низкочастотного усилителя УНЧ, блока питания и полуактивного имитатора аудиотранспондера. Связь управляющей ПЭВМ

Рис. 2.51. Регистратор модуляции вторичного излучения «Ревиз-5000»

с основным блоком устройства осуществляется по средствам USB-кабеля. ПЭВМ осуществляет управление генератором ВЧ и приемником. Зондирующий сигнал в диапазоне частот 30...5000 МГц формируется генератором ВЧ. В комплексе «Ревиз-5000» реализована возможность выбора двух схем работы: с использованием одной приемо-передающей (встроенной) антенны; с двумя внешними (приемной и передающей) антеннами. Коммутация осуществляется с помощью разъемов «АО», «А1» и «П1», «А2» и «П2». С выхода генератора через усилитель мощности и направленный ответвитель зондирующий сигнал передается на встроенную широкополосную направленную антенну и излучается в окружающее пространство. Отраженный сигнал принимается той же антенной и через другой выход направленного ответвителя поступает на вход приемника. Направленный ответвитель обеспечивает разделение зондирующего и принимаемого сигнала. Подключение внешних широкополосных антенн осуществляется посредствам разъемов «А1» и «А2». Приемник перестраивается синхронно с генератором и служитдля выделения модуляции принимаемого сигнала. С выхода «21-11304 Гц» сигнал модуляции в диапазоне 21...11304 Гц поступает на ПЭВМ и УНЧ. Выход «АНАЛИЗАТОР» служит для подключения внешнего анализатора спектра для анализа модулирующего сигнала в диапазоне частот 0 - 1000 МГц. УНЧ служит для вывода сигнала модуляции на головные телефоны и имеет регулятор «ГРОМКОСТЬ». Разъем «НАУШНИКИ» служит для подключения головных телефонов (наушников).

Блок питания служит для формирования питающих напряжений. Питание может осуществляться как от сети переменного напряжения (220 В, 50 Гц), так и от встроенных аккумуляторных батарей. При подключении сетевого шнура к разъему «220В/50Гц» и включении выключателя «О/I» осуществляется зарядка аккумуляторных батарей основного устройства. Подача питающих напряжений на остальные блоки устройства осуществляется автоматически при включении ПЭВМ, подключенной к устройству. При выключенном выключателе «О/I» или отсоединенном сетевом шнуре питание осуществляется от встроенных аккумуляторов.

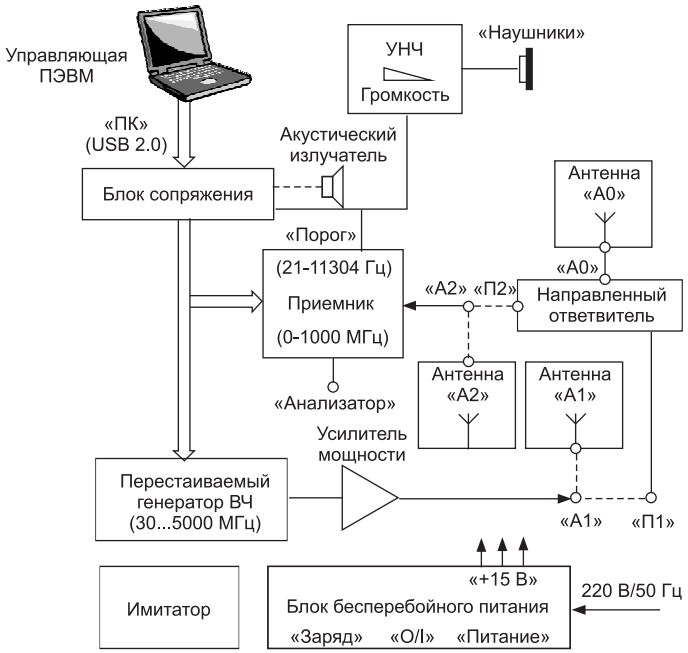


Рис. 2.52. Функциональная схема комплекса «Ревиз-5000»

Основные технические характеристики: рабочий диапазон частот 30...5000 МГц; минимальный шаг перестройки частоты внутреннего генератора 100 кГц; чувствительность приемного устройства аппаратуры не хуже −110 дБВт при отношении сигнал/шум 10 дБ в полосе пропускания 10 кГц; динамический диапазон анализируемого НЧ сигнала не менее 116 дБ; выявление модуляционных информативных сигналов с коэффициентом модуляции не хуже 1×10, в полосе акустических сигналов 180...11300 Гц, для которых отношение сигнал/шум превышает 10 дБ. На расстоянии 1 метр аппаратура позволяет обнаруживать аудиотранспондеры с максимальной дальностью возможного облучения не менее 20 метров.

Перестройка по частотному диапазону может осуществляться как автоматически, так и вручную оператором. Время перестройки во всем рабочем диапазоне частот в автоматическом режиме при стандартных настройках параметров программного обеспечения не более 12 минут.

Аппаратно-программный комплекс «Омега-АМ» (рис. 2.53). Для выполнения задачи по обнаружению и локализации объектов, обладающих свойствами эндовибрации, был разработан аппаратно-программный комплекс для исследования модуляции переизлученных колеба-

Рис. 2.53. Комплекс для исследования модуляции переизлученных колебаний «Омега-АМ»

ний «Омега-АМ». Комплекс представляет собой комплект оборудования, предназначенный для обнаружения резонансных переизлучателей (эндовибраторов и других вторичных излучателей) в технических средствах обработки информации, средствах оргтехники, помещениях, предметах интерьера и т. п. Принцип работы изделия основан на том, что обследуемые объекты облучаются высокочастотным электромагнитным полем (100...3000 МГц) при одновременном акустическом воздействии. Переизлученный (отраженный) сигнал принимается на приемную антенну и анализируется на наличие модуляции, обусловленной этим акустическим воздействием. При этом во всем рабочем диапазоне обеспечивается заданная чувствительность и максимальное значение подводимой к антенне мощности облучаемого сигнала.

В состав комплекса входят управляемый высокочастотный генератор, приемная и передающая антенны, акустический излучатель, широкодиапазонный эталонный переизлучатель, который содержит три переизлучающие структуры с резонансными частотами 500, 1000 и 2250 МГц.

Управление аппаратурой и обработка результатов осуществляется с помощью многофункционального комплекса радиоконтроля «Омега». Комплекс может работать в автоматическом и ручном режимах. В автоматическом режиме комплекс облучает исследуемый объект высокочастотным электромагнитным полем и выполняет обнаружение и измерения относительных уровней модуляционных сигналов в переизлученных колебаниях, обусловленных акустическим воздействием на объект. Исследования выполняются при последовательном сканировании заданного диапазона радиочастот с равномерным или переменным шагом по частоте с параметрами, которые предварительно вводятся при настройке программы. Для исключения влияния фазового шума генератора и гетеродинов приемника, обнаружение и измерение уровней модуляционных сигналов выполняется с помощью анализатора спектра огибающей, полоса обзора которого может расширяться до 100 кГц. Это позволяет регистрировать высокочастотные модуляционные компоненты в спектре отраженного сиг-

нала. После завершения сканирования все результаты сохраняются в файле и могут быть представлены в виде документального отчета.

В ручном режиме для проведения исследований оператор использует панорамный анализатор спектра, отражающий внешнюю радиообстановку в месте измерений, а также цифровые анализаторы спектров и огибающих принимаемых сигналов. В процессе измерения оператор может изменять частоту и мощность излучаемого сигнала, частоту и уровень акустического воздействия, частоту модуляции эталонного переизлучателя, чувствительность радиоприемника и параметры отображения спектров. Чувствительность комплекса ограничена уровнем собственных шумов анализатора спектра огибающей, который соответствует коэффициенту амплитудной модуляции (относительно амплитуды принимаемого сигнала) около $6 \cdot 10^{-5}$.

В процессе визуального осмотра ограждающих конструкций, мебели и других предметов интерьера помещений, как правило, выявляется большое количество мест, вызывающих подозрение по тем или иным внешним признакам. Далеко не всегда возможно или целесообразно рассеять возникшие подозрения с помощью взлома стены, мебельной панели или вскрытия пола. Во всех этих случаях более рациональным считается применение специальных технических средств неразрушающего контроля:

- приборов нелинейной радиолокации;
- обнаружителей пустот;
- металлодетекторов;
- флуороскопов;
- рентгенотелевизионных комплексов.

2.6. Нелинейные локаторы

Свойства электропроводящих материалов отражать радиоволны были положены в основу радиолокационного обнаружения. Этими свойствами в полной мере обладают электронные средства перехвата информации. Поскольку для опознавания объектов используются нелинейные свойства полупроводниковых схемных элементов, данный вид локации назвали нелинейной, а приборы — нелинейными локаторами.

2.6.1. Принцип работы нелинейного локатора

В состав нелинейного локатора (НЛ) входят передатчик, приемник, приемо-передающая антенная система, устройства индикации.

Способность локатора обнаруживать объекты, содержащие электронные компоненты, основана на следующем. Любые радиоэлектронные устройства (РЭУ) состоят из печатных плат с проводниками, которые могут служить антеннами. К ним подключены полупроводниковые элементы: диоды, транзисторы, микросхемы, представляющие

для высокочастотного зондирующего сигнала локатора набор нелинейных отражателей. В результате облучения на этих антеннах наводятся высокочастотные переменные ЭДС. Элементами с нелинейной вольт-амперной характеристикой они преобразуются в сигналы кратных частот (гармоники), переизлучаемые в пространство. Переизлученный сигнал поступает на вход приемного устройства локатора, настроенного на частоты гармоник 2-го и 3-го порядка. По наличию в спектре принимаемого сигнала высшей гармоники удвоенной частоты собственного передатчика устанавливается факт присутствия в зоне зондирования любого РЭУ независимо от того, включено оно или выключено.

Помехами для нелинейного локатора могут быть отражения от соприкасающихся металлических поверхностей. При контакте таких слоев возникает полупроводниковый нелинейный элемент с неустойчивым p-n-переходом. В физике полупроводников такое образование известно как металл–окисел–металл, а возникающий элемент называется МОМ-диод. МОМ-структура преобразует спектр зондирующего сигнала в частотный спектр, отличающийся от спектра сигнала, отраженного от электронного элемента. Различие обусловлено временно́й и механической нестабильностью МОМ-структуры и проявляется в соотношении уровней компонентов спектра, являющихся продуктами нелинейных преобразований второго и третьего порядка, при этом будут преобладать гармоники третьего порядка. Источником помех могут служить и радиопередатчики, работающие на частотах, близких или кратных частоте зондирующего сигнала.

Главное достоинство нелинейных локаторов — способность обнаруживать электронные схемы как во включенном, так и выключенном состоянии, недостаток — сравнительно большое число «ложных» обнаружений естественных нелинейных отражателей типа МОМ.

2.6.2. Эксплуатационно-технические характеристики локаторов

Основными параметрами, используемыми при сравнении эксплуатационных качеств нелинейных локаторов, являются: режим работы, мощность и частота зондирующего излучения передатчика, чувствительность приемника, направленные свойства антенной системы, точность устройств индикации, а также сервисные возможности приборов.

В зависимости от режима работы передатчика различают нелинейные локаторы непрерывного и импульсного излучения. Мощность излучения в значительной степени определяет коэффициент преобразования ($K_{\text{п}}$) энергии зондирующего сигнала в энергию высших гармоник. Повышение мощности улучшает характеристики нелинейных

локаторов, но одновременно приводит к увеличению опасного воздействия на оператора. Средняя мощность локаторов непрерывного излучения от 0,3 до 3 Вт. Пиковая мощность импульсных нелинейных локаторов, при сравнимой или меньшей средней, от 150 до 400 Вт, т. е. почти на 30 дБ превышает мощность приборов непрерывного излучения.

Так как эффективность преобразования определяется не средней мощностью излучения, а ее пиковым значением, дальность действия локаторов, работающих в импульсном режиме, оказывается выше, чем у приборов с непрерывным излучением, при прочих равных условиях.

Чем выше частота излучения, тем меньше геометрические размеры антенной системы, тем удобнее работа с прибором. Но с увеличением частоты по экспоненциальному закону растет доля энергии, поглощаемой материальной средой, укрывающей средство съема. Вместе с тем при приближении частоты излучения НЛ к рабочей частоте закладки из-за околорезонансных явлений возрастает уровень переотражённых сигналов и, следовательно, вероятность ее обнаружения. Приборы, предлагаемые в настоящее время, работают в частотном диапазоне 680...3600 МГц. Чувствительностью приемника определяется максимальная дальность действия НЛ. Для современных приборов этот показатель составляет от -110 до -145 дБ.

Передающие устройства локаторов, генерирующие зондирующий сигнал, характеризуются:

- режимом работы (непрерывным или импульсным);
- пределами регулирования выходной мощности, дБ;
- частотой непрерывного излучения;
- частотой следования и длительностью радиоимпульса, мкс.

Качество приемного устройства, регистрирующего переизлученные сигналы, отражается следующими показателями:

- частотами настройки, МГц, на регистрируемые гармоники (2 и 3);
- реальной чувствительностью при определенном соотношении сигнал/шум, дБ·Вт;
- пределами регулирования чувствительности, дБ.

Основными параметрами антенной системы, излучающей зондирующие сигналы и принимающей переотраженные излучения на частотах высших гармоник, являются:

- коэффициент направленного действия (КНД);
- ширина главного лепестка диаграммы направленности по уровню половинной мощности, град;
- уровень подавления задних лепестков диаграммы направленности, дБ;

- коэффициент эллиптичности (для антенн с круговой поляризацией).

Эксплуатационные показатели локаторов определяются во многом качеством устройств индикации режимов работы и параметров сигналов. Большинство современных нелинейных локаторов оборудованы многосегментными светодиодными индикаторами и звуковыми сигнализаторами переменного тона.

2.6.3. Методика работы с локатором

Нелинейный локатор выполняет три основные функции: обнаружение нелинейных отражателей, определение местоположения и идентификацию средства съема информации.

Зондирующее излучение легко проникает во многие материалы, мебель, может проходить (с ослаблением) через внутренние перегородки помещений, бетонные стены и полы.

Обнаружительная характеристика нелинейного локатора нормируется только для свободного пространства. В условиях поиска закладочных устройств (ЗУ) речь идет не о дальности, а о максимальной глубине обнаружения объектов в маскирующей среде. Оценка ведется по уровню отклика, увеличивающемуся при приближении к объекту, что позволяет определить точное местоположение ЗУ.

При работе на открытых площадях или в больших необорудованных помещениях импульсные локаторы могут обеспечить в несколько раз большую дальность обнаружения, чем непрерывные, что позволяет сократить время обследования. При работе в офисах максимальная дальность локаторов обоих типов практически не используется из-за насыщенности выделенных и соседних помещений электронной техникой и контактными помеховыми объектами.

Реальная дальность в этих случаях примерно 0,5 м для локаторов любого типа. Она регулируется оператором с учетом помеховой обстановки снижением мощности передатчика или загрублением чувствительности приемника до предела, позволяющего различать, от какого объекта пришел отклик. Дальность зависит от типа обнаруживаемого устройства (например, закладка с большей по длине антенной, как правило, обнаруживается на более значительном расстоянии) и условий его размещения (в мебели, за преградами из дерева, кирпича, бетона и т. д.).

Итак, для решения первого этапа поисковых мероприятий, обнаружения средств съема информации, оператору необходимо проделать следующие операции:

- включив НЛ, обнаружить и по возможности устранить источники мешающих сигналов;

- установить максимальный уровень чувствительности приемного устройства и максимальный уровень мощности передатчика зондирующего сигнала;
- сканированием ограждающих конструкций и предметов интерьера с расстояния примерно 1 м провести контроль помещения на наличие мощных помеховых объектов, как «коррозийных», так и электронных (в основном электронная оргтехника и радиоаппаратура).

При этом назначение объектов должно быть точно установлено, и они должны быть либо удалены из помещения, либо не приниматься во внимание при дальнейшем поиске. Следует учитывать, что эти помеховые объекты могут находиться в соседних комнатах и на других этажах, которые при необходимости и возможности целесообразно осмотреть. После удаления из комнаты источников сильных помех повторить осмотр стен, потолков, мебели и приборов с расстояния 20 см и меньше. В ходе осмотра отметить подозрительные зоны.

Определение местоположения осуществляется с помощью оценки уровня и пеленга сигнала отклика. Под пеленгом понимается направление, соответствующее максимальному уровню принимаемого сигнала. Следует учитывать, что зондирующие и отраженные сигналы переотражаются близлежащими объектами. Эффективными рефлекторами являются зеркала, металлические плиты, сетки, арматура и т. д. При их облучении можно регистрировать переотраженные сигналы от нелинейных отражателей, находящихся за спиной оператора.

Для определения точного местоположения средств съема информации необходимо:

- снизить уровень излучаемой мощности и чувствительность приемника;
- перемещая антенну около подозрительных зон, анализировать показания светового индикатора и частоту тонального сигнала в головных телефонах;
- определить направление прихода отраженного сигнала максимального уровня, взять пеленг по ориентации антенны;
- определив точное местоположение, приступить к идентификации объекта.

Для исключения ошибки при сравнении показаний индикаторов необходимо по мере достижения любым из светодиодных столбцов максимальной высоты уменьшать чувствительность приемника или снижать мощность передатчика так, чтобы засвеченный шлейф не доходил на один–три сегмента до предела шкалы.

Для четкой идентификации «коррозийных диодов» и полупроводников существует ряд методов, позволяющих достигать высокого практического эффекта.

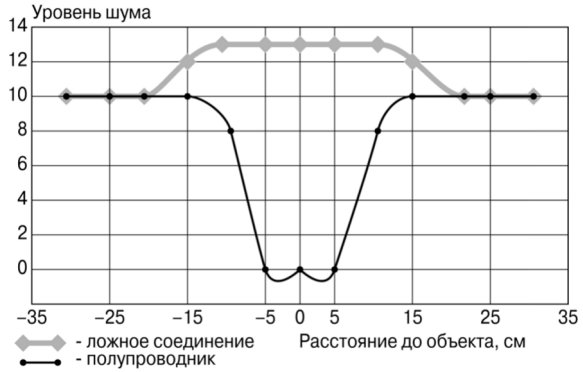


Рис. 2.54. Изменение уровня шума в районе p-n-перехода

В приборах, принимающих сигналы отклика одновременно на второй и третьей гармониках зондирующего сигнала, идентификация объекта проводится сравнением уровней сигналов на выходах обоих трактов приема. При облучении полупроводникового соединения возникает сильное переотражение зондирующего сигнала на частоте 2-й гармоники и слабое на частоте 3-й. МОМ-диод ведет себя иначе, создавая сильное переотражение на 3-й и слабое на 2-й гармониках.

В ряде приборов предусмотрена возможность «прослушивания» демодулированных сигналов гармоник, позволяющая идентифицировать объект, используя эффект изменения уровня шума. По мере приближения антенны нелинейного локатора к p-n-переходу отмечается значительное понижение уровня шума, достигающего минимума непосредственно над объектом. При облучении МОМ-диодов этот эффект практически не наблюдается (рис. 2.54).

Однако существуют ложные соединения, также снижающие уровень шума, как и p-n-переход. Для их выявления рекомендуется произвести механическое воздействие на подозрительное место.

Любое механическое воздействие приводит к изменению геометрии МОМ-диода и его преобразующих свойств. На практике механическое воздействие осуществляется вибрационным методом, при этом в преобразованном сигнале ясно прослушивается частота вибрации. Уровень вибрации может быть минимальным, поэтому достаточно легкого постукивания рукой по обследуемой поверхности. Даже если модель локатора рассчитана на прием 2-й и 3-й гармоник, данная операция позволяет более точно идентифицировать объект.

В большинстве моделей импульсных нелинейных локаторов предусмотрен так называемый режим «20К». Суть данного режима в том, что подается дополнительный зондирующий сигнал с частотой следования зондирующих импульсов 20 кГц. Звуковой сигнал, полу-

ченный при детектировании выделенной огибающей переизлученного сигнала от исскуственного p-n-перехода, лежит за пределами восприятия человеческого уха.

Однако при неустойчивом МОМ-контакте не все зондирующие импульсы переотражаются, т. е. выделяется огибающая, соответствующая более низкой частоте, которая слышна в наушниках как шумовой сигнал.

Для повышения точности идентификации объекта в нелинейных локаторах предусматриваются режимы приема на частотах 2-й и 3-й гармоник зондирующего излучения, а также прослушивания сигналов, транслируемых средствами съема за пределы обследуемого помещения.

Рассмотрим основные характеристики современных нелинейных локаторов.

2.6.4. Современые нелинейные локаторы

Локатор нелинейностей «Люкс» (рис. 2.55) является высокоэффективным поисковым средством, предназначенным для обнаружения радиоэлектронных устройств, а также отдельных полупроводниковых элементов вне зависимости от места их расположения. В ходе работы прибор генерирует микроволновое излучение, которое при попадании на транзистор, диод или микросхему переизлучается на частотах 2-й и 3-й гармоник.

Принимаемые антенной сигналы поступают на блок обработки. По светодиодным индикаторам производится отсчет уровней принятых сигналов на 2-й и 3-й гармониках. Разрешающая способность индикаторов 3 дБ. Сигналы можно также прослушать через подключаемые к штанге прибора головные телефоны. Режим «20K» позволяет прослушивать низкочастотный сигнал работающего устройства — магнитофона, радиопередатчика, микрофонного усилителя и является мощным инструментом для получения более качественной информации о типе нелинейного элемента. В этом режиме сигналы на

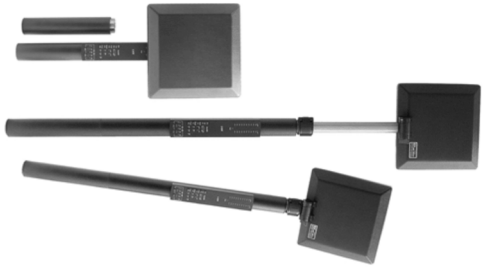


Рис. 2.55. Общий вид локатора нелинейностей «Люкс»

частотах гармоник, принимаемые изделием, оказываются промодулированы низкочастотным сигналом, имеющимся в электронных цепях обнаруженного или исследуемого устройства. Система автоматического выбора оптимальной частоты (отстройка от GSM) позволяет локатору работать в условиях сосредоточенных помех. Предусмотрена возможность регулировки мощности передатчика и чувствительности приемников. Радиолокатор работает в импульсном режиме с мощностью излучения 16 Вт в импульсе. Это позволяет обеспечить высокую (−130 дБВт) чувствительность приемников. По дальности обнаружения прибор не уступает самым мощным выпускаемым на сегодняшний день радиолокаторам. Это обеспечивается оптимально подобранными параметрами излучения и приема в сочетании с эффективной антенной системой.

«Люкс» выполнен в виде неразборной конструкции, состоящей из антенного блока и ручки-штанги, соединённых шарниром. В ручке размещаются передатчик, два приемника, блоки обработки и индикации данных. На лицевой панели прибора расположены кнопки управления и светодиодные индикаторы. Блок аккумуляторов присоединяется к корпусу изделия при помощи резьбового соединения.

Оригинальная конструкция контактов обеспечивает надежное питание прибора в любых условиях его эксплуатации. На торцевой грани аккумуляторного блока расположены разъёмы подключения зарядного устройства и головных телефонов. Для первоначальной настройки локатора используется имитатор нелинейности (2-я и 3-я гармоники), поставляемый в комплекте с изделием. Небольшие габариты, эргономичная конструкция, а также вес локатора, не превышающий 1,3 кг, позволяют использовать его в самых сложных условиях. Важной особенностью изделия является отсутствие дополнительных блоков, присоединяемых на разъемах, что, как правило, ведет к снижению надежности устройства и создает неудобства для оператора. Передатчик работает в импульсном режиме в диапазоне 915 МГц. Шаг перестройки частоты 200 кГц. Максимальная выходная мощность в импульсе 16±1 дБ. Минимальная выходная мощность в импульсе 1,6 дБ. Частоты настроек приемников равны удвоенной и утроенной частоте передатчика соответственно. Реальная чувствительность каждого приемника при соотношении сигнал/шум не менее 6 дБ составляет −136 дБ/Вт. Динамический диапазон приемников не менее 30 дБ. Регулировка усиления приемников осуществляется вручную, четырьмя ступенями по 10±1 дБ в каждой ступени. В режиме «20K» приемники выделяют сигналы, которыми модулируется по амплитуде последовательность радиоимпульсов. Ширина спектра демодулированнного сигнала 500...2000 Гц. Изделие имеет три антенны, конструктивно

Рис. 2.56. Локатор нелинейности NR-μ

Рис. 2.57. Нелинейный радиолокатор NR-900EMS

оформленные в виде одного блока. Ширина диаграммы направленности главного лепестка по уровню −3 дБ передающей и приемных антенн не более 90°. Уровень мощности боковых и задних лепестков диаграммы направленности передающей и приемных антенн не более 10 % от уровня главного лепестка. Передающая и приемные антенны имеют круговую поляризацию с коэффициентом эллиптичности не более 1,5. Передающая и приемные антенны имеют соосные диаграммы направленности. Отклонения максимумов главных лепестков диаграмм направленности не превышает 50. Длительность непрерывной работы прибора не менее 5 часов. Время подзарядки аккумуляторов 1,5 часа.

Нелинейный радиолокатор NR-μ (рис. 2.56). Оригинальные схемотехнические решения, реализованные в приборе, позволяют оптимальным образом использовать преимущества как импульсных, так и непрерывных локаторов. Возможность перестройки частоты зондирующего сигнала помогает адаптировать прибор к сложной помеховой обстановке.

Основные ТТХ: рабочая частота 848 МГц; выходная мощность не менее 2 Вт (средняя 0,4 Вт); регулировка 10 дБ (с шагом 5 дБ); модуляция: амплитудно-импульсная (поиск), CW («20k»); прием отклика по 2-й и 3-й гармоникам; чувствительность не хуже −150 дБ/Вт (с учетом цифровой обработки; аттенюатор от −10 до −40 дБ (с шагом 10 дБ); поляризация — круговая; индикация звуковая, визуальная; питание: аккумулятор 6 В (ресурс 5 ч). Особенности: компактная конструкция; возможность частотной отстройки от внешних помех; удобное управление; цифровая обработка сигнала; сочетание достоинств импульсного и непрерывного режимов.

Нелинейный радиолокатор NR-900EMS (рис. 2.57) предназначен для обследования элементов строительных конструкций и предметов интерьера. Применяется для выявления и локализации скрыто установленных средств негласного съема информации, в том числе дикто-

фонов и другой аппаратуры, содержащей полупроводниковые радиоэлементы. При этом не имеет значения, находятся ли эти устройства в режиме передачи, выключенном или сторожевом режимах. Высокий энергетический потенциал позволяет использовать детектор для дистанционного обнаружения самодельных взрывных устройств с приемниками дистанционного управления или электронными таймерами.

Прибор обладает высокой помехозащищенностью, невосприимчивостью к сигналам сотовой связи любых стандартов. Имеет режим выделения огибающей (20K). Средняя мощность СВЧ сигнала не более 0,2 Вт. Ступенчатая регулировка выходной мощности сигнала 8 дБ. Несущая частота 848 МГц. Чувствительность двухканального приемника не хуже −150 дБВт. Поляризация антенн круговая. Индикация визуальная и звуковая. Время непрерывной работы прибора от встроенного аккумулятора не менее 8 часов в режиме поиска и не менее 4 часа в режиме 20K. Масса снаряженного блока приемопередатчика (со встроенным аккумулятором) не более 2,2 кг. Масса телескопической штанги с антенной системой и пультом индикации и управления не более 1,5 кг.

Рис. 2.58. Нелинейный радиолокатор NR-2000

Нелинейный радиолокатор NR-2000 (рис. 2.58) предназначен для выявления мобильных телефонов и SIM карт; обнаружения электронных устройств негласного съема информации; поиска самодельных взрывных устройств (электронных систем управления СВУ) на фоне сложной техногенной помехи от городской застройки. Прибор имеет амплитудно-импульсную модуляцию. Может работать в режимах работы «Поиск» и «20K». Средняя мощность СВЧ сигнала в режиме поиска не более 200 мВт. Излучаемая мощность (ERP) не менее 700 Вт. Возможна плавная регулировка выходной мощности зондирующего сигнала до −15 дБ с шагом 1 дБ; обнаружение радиоэлектронных устройств за армирующими строительными конструкциями; уверенное обнаружение малоразмерных целей в различных, в том числе и во влажных средах. Моноблочная конструкция (ружейная компоновка «булпап»), отсутствие разъемных соединений и кабелей, антенная система на раздвижной штанге, подсветка зоны поиска делают прибор компактным и удобным в использовании как в помещениях, так и при обследовании больших площадей на местности. Прибор позволяет обнаруживать мобильный телефон с расстояния более 1 м, SIM (UIM)-карту с расстояния около метра.

Нелинейный локатор «Кайман» ST 400 (рис. 2.59) предназначен для обнаружения электронных устройств перехвата информации мобильных телефонов и SIM-карт иных электронных устройств, содержащих полупроводниковые элементы при проведении поисковых работ.

Рис. 2.59. Нелинейный локатор «Кайман» ST 400

ST 400 позволяет обнаружить как включенные, так и выключенные электронные устройства, а также точно определить их место установки. Используя локатор, оператор может отличить отклики реальных полупроводников от ложных сигналов (коррозия, металл, структура металл–окисел–металл). Диапазон рабочих частот 2...3 ГГц. Максимальная пиковая излучаемая мощность не более 2 Вт. Прибор может работать в следующих режимах: ручном, автоматическом, аудио, адаптации. Наличие аудиорежима позволяет прослушивать демодулированные сигналы. Диапазон изменения усиления приемника и регулировки чувствительности в ручном режиме 40 дБ (пять шагов по 8 дБ). Световая индикация уровня принимаемого сигнала обеспечивается тремя 16-сегментными шкалами, звуковая — встроенными динамиком и наушниками. Прибор имеет четырёхсекционную телескопическаю штангу и изменяемый наклон антенного модуля прибора. Время непрерывной работы от полностью заряженного аккумулятора от 6 до 8 часов.

Двухдиапазонный нелинейный радиолокатор «Лорнет-0836» (рис. 2.60) предназначен для поиска и обнаружения электронных устройств, находящихся как в активном, так и в выключенном состоянии. Прибор является дальнейшим развитием локаторов семейства «Лорнет» и в нём впервые в мировой практике реализована концепция одновременного использования для зондирования контролируемых объектов, излучений двух частототных диапазонов: 800 и 3600 МГц. Это дает данному изделию неоспоримое преимущество перед одночастотными приборами, так как:

- на высокой частоте лучше искать мелкие и высокочастотные полупроводниковые устройства (и наоборот);
- во влажном грунте, в бетонных стенах лучше работать на низкой частоте;
- наличие двух антенн с широкой (на низкой частоте) и узкой (на высокой частоте) диаграммами направленности позволяет сначала быстро оценить обстановку (на низкой частоте), а затем, используя высокую частоту, точно локализовать объект.

Рис. 2.60. Двухдиапазонный нелинейный радиолокатор «Лорнет-0836»

Рис. 2.61. Досмотрово-поисковый локатор «Лорнет-24»

Локатор автоматически выбирает наилучший частотный канал приема, свободный от помех, что позволяет работать с прибором в сложной электромагнитной обстановке.

Применение параболической антенны, обладающей большим коэффициентом усиления (20 дБ на частоте 3600 МГц) позволило увеличить дальность обнаружения нелинейных элементов и обеспечить их точную локализацию в пространстве. Для удобства оператора локатор снабжен лазером, подсвечивающим место, на которое направлена антенна.

В локаторе предусмотрены два вида излучаемых сигналов с импульсной модуляцией несущей частоты со скважностью 280 (Pulse) и 16 (CW).

Режим CW предназначен для прослушивания огибающей принятого сигнала на встроенный динамик (или наушники), что может быть использовано для выявления работающих аналоговых радиомикрофонов за счет возникновения акустозавязки.

Наличие режима автоматического регулирования выходной мощности существенно облегчает работу оператора.

На светодиодном индикаторе обнаружителя отображаются одновременно уровни сигналов второй и третьей гармоник передатчиков. Оператор может производить поиск как на одной из частот (низкой или высокой), так и на двух сразу. В случае выбора двухчастотного режима работы на индикаторах отображается уровень сигнала того приемника, который в данный момент больше.

Кроме того, уровень второй гармоники можно оценивать на слух по частоте следования щелчков, воспроизводимых через встроенный громкоговоритель или беспроводные наушники.

Досмотрово-поисковый локатор «Лорнет-24» (рис. 2.61) используется при проведении оперативно-поисковых работ в помещениях,

в автомашинах, досмотре людей и бандеролей, обнаруживает технические средства и устройства, имеющие в своём составе полупроводниковые компоненты.

Локатор оснащен системой автоматического выбора частот и может автоматически отстраиваться от сосредоточенных помех (по критерию минимального шума в канале приёма 2-й гармоники). Основные характеристики: малые габариты (умещается в кармане), не имеет мировых аналогов; простота в работе, удобный прибор для досмотра: сохранены все режимы изделия «Лорнет» (автоматическое и ручное изменения мощности зондирующего сигнала в импульсном режиме, ручное изменения мощности в непрерывном режиме); использование новейших технологий и материалов, эргономичность; электромагнитное воздействие на человека (при досмотре) значительно ниже, чем воздействие сотового телефона; высокий обнаружительный потенциал (из-за более высокой частоты зондирующего сигнала в некоторых случаях оказывается более эффективным по сравнению с локаторами, работающими с большей мощностью, но в стандартном диапазоне); использование беспроводных наушников; удобство работы в труднодоступных местах, в условиях ограниченного пространства, в автомашине (толщина антенны не превышает 18 мм).

Портативный детектор нелинейной локации «Буклет-2» (рис. 2.62) предназначен для обнаружения электронных компонентов, как активных, так и пассивных, замаскированных в различных средах. Индикация выявленных радиоэлектронных устройств обеспечивается через светодиодный индикатор, расположенный на корпусе устройства, либо через подключаемые наушники.

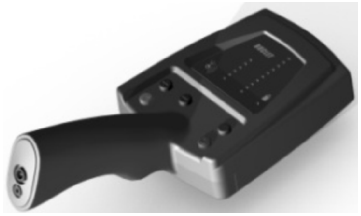


Рис. 2.62. Общий вид детектора нелинейной локации «Буклет-2»

Дальность обнаружения приемо-передающего оборудования и радиоэлектронных устройств, в том числе таких, как SIM-карты сотовых телефонов, диктофоны и других, зависит от типа обнаруживаемого устройства и составляет от 10 см до нескольких метров.

Особенностями «Буклета-2» являются: уникальный дизайн и эргономичность; малые габариты и вес (не более 350 г); высокое качество демодуляции принятого сигнала. Использование диапазона излучения 2400 МГц позволяет работать без помех, мешающих работе нелинейных локаторов работающих в диапазоне 850...950 МГц. Прибор может использоваться в качестве досмотрового устройства и обладает следующими техническими характеристиками: непрерывный зондирующий сигнал; эффективная излучаемая мощность 0,5 Вт; чувствительность приемников −150 дБВт; диапазон излучения 2400 МГц;

Рис. 2.63. Комбинированное устройство «Буклет-МД»

автоматический выбор свободного канала; динамический диапазон 80 дБ; плотность потока энергии, создаваемая прибором в направлении излучения не выше 200 мкВт/см^2; излучающая и приемные антенны имеют круговую поляризацию с коэффициентом эллиптичности не хуже 1,5; габариты изделия 220×90×90(30) мм; питание — Li-Ion аккумулятор; время непрерывной работы не менее 3,5 ч; автоматический контроль разряда батареи; время подзарядки 1 ч; диапазон рабочих температур от −10 до +40 °С.

В настоящее время на рынке информационных услуг появляются универсальные приборы, сочетающие в себе функции нелинейного локатора и металлодетектора. Один из представителей таких приборов — «Буклет-МД» (рис. 2.63).

Изделие «Буклет-МД» является комбинированным устройством, имеющим двойное функциональное предназначение: металлодетектора и обнаружителя электронных компонентов (нелинейного локатора). При этом нелинейный локатор размещается внутри стандартного корпуса ручного досмотрового металлодетектора. Визуальные признаки наличия в устройстве локатора отсутствуют. Индикация выявленных радиоэлектронных устройств обеспечивается через штатные индикаторы металлодетектора. Изделие «Буклет-МД» обеспечивает обнаружение радиоэлектронных устройств, таких как сотовые телефоны, диктофоны, приемо-передающее оборудование, и их элементов, которые могут находиться под одеждой на теле человека или в личных вещах на расстоянии не менее 10 см. Функции металлодетектора в изделии сохраняются.

Изделие размещено внутри штатного корпуса металлодетектора «Гаррет» и состоит из двух отдельных блоков — металлодетектора и нелинейного локатора. Включение изделия осуществляется нажатием кнопки, расположенной на боковой поверхности под индикаторами. О готовности изделия к работе свидетельствует зеленый индикатор. Красный светодиод является индикатором металлодетектора и включается при попадании в его зону действия металлического предмета. Желтый светодиод является индикатором нелинейного локатора и включается при попадании в зону действия устройства радиоэлектронных компонентов. Оба блока смонтированы в различных частях корпуса, поэтому при работе с устройством необходимо учитывать расположение эффективных рабочих зон металлодетектора и нелинейного локатора. Кроме того, если металлодетектор работает одинаково эффективно при любом положении устройства, то рабочая зона нелинейного локатора находится с той стороны устройства, на которой расположена штатная табличка со штрихкодом, инструкций и указателями кнопок.

Технические характеристики: диапазон рабочих температур от +5 до +40 °С; вес изделия не более 1 кг (суммарный вес с учетом веса штатного изделия); габариты изделия 8,3×4,13×42 см; питание — Li-Ion аккумулятор 1,2 а/ч×7,2 В; время непрерывной работы не менее 3 часов; автоматический контроль разряда батареи; время полной зарядки 2,5 часа; разъем для подключения наушников/зарядки аккумулятора. Характеристики нелинейного локатора, используемого в комбинированном устройстве: эффективная излучаемая импульсная мощность 1 Вт ±1,5 дБ; чувствительность приемников −120 дБм; плотность потока энергии, создаваемая прибором в направлении излучения, не выше 200 мкВт/см^2. Характеристики металлодетектора, используемого в комбинированном устройстве: рабочая частота 93 кГц; оптимальная дистанция для обнаружения металлического предмета 10...15 см; световая и звуковая индикация тревоги; настройка автоматическая.

2.7. Досмотровая техника

Для выявления внедренных устройств перехвата информации как объектов, имеющих определенные физические свойства (габариты, массу, структуру и т. д.), применяют досмотровые технические средства.

2.7.1. Металлодетекторы

Электронные средства съема информации обнаруживают в маскирующих средах методом вихретокового контроля, который заключается в анализе взаимодействия внешнего электромагнитного (ЭМ)

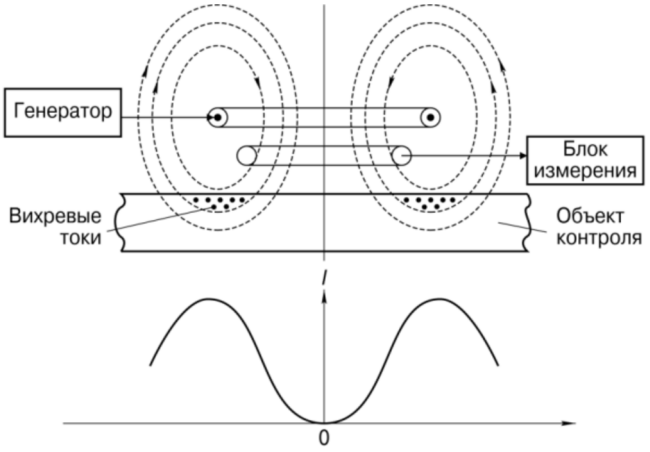


Рис. 2.64. Принципиальная схема вихретоковых преобразователей

поля с ЭМ полем вихревых токов, наводимых только в электропроводящих объектах. Распределение и плотность вихревых токов определяются источником ЭМ поля, геометрическими размерами и электромагнитными свойствами объекта, а также их взаимным расположением. В качестве источника ЭМ поля чаще всего используется индуктивная катушка, называемая вихретоковым преобразователем (ВТП). В современных приборах применяют двухкатушечные ВТП. Одна катушка — возбуждающая, служит для создания вихревых токов в объекте, а другая — измерительная, для измерения ЭДС, наводимой результирующим магнитным потоком, проходящим внутри измерительной катушки (рис. 2.64).

Достоинством вихретоковых металлодетекторов является то, что контроль можно осуществлять без непосредственного контакта с объектом, в том числе и при движении катушки относительно маскирующей среды с достаточно высокой скоростью. Дополнительное преимущество заключается в том, что на сигналы ВТП не влияют влажность, давление, загрязнение воздушной среды и поверхности объекта, радиоактивные излучения.

В поисковых операциях применяют в основном ручные металлодетекторы, снабженные световыми и звуковыми индикаторами.

Модели АКА-7215 «Унискан» осуществляют селекцию объектов из черных и цветных металлов, снабжены системой игнорирования мелких предметов из ферромагнитных материалов, имеют высокую чувствительность, позволяющую обнаруживать пистолет Макарова, отличая его от сигаретной алюминиевой фольги.

Самая миниатюрная модель АКА-7210 «Минискан» (рис. 2.65) имеет габариты 160 ×80×30мм, что позволяет использовать ее в

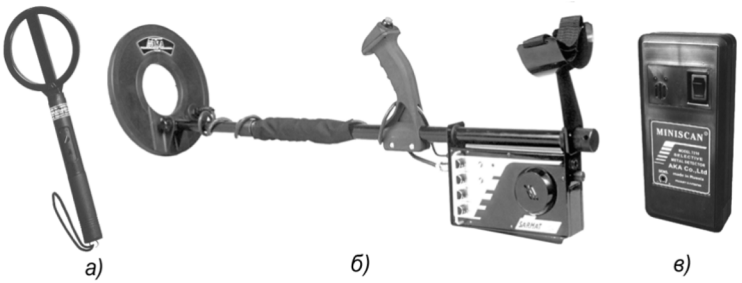


Рис. 2.65. Общий вид металлодетекторов: *а* — АКА-7202; *б* — АКА-7240; *в* — АКА-7210 «Минискан»

Рис. 2.66. Общий вид металлодетектора типа «Сфинкс»

скрытоносимом варианте для обнаружения оружия. Селекция объектов из черных и цветных металлов сочетается в этом приборе с высокой чувствительностью.

Профессиональный высокочувствительный компьютеризированный селективный грунтовой металлодетектор АКА-7234 «Стерх Мастер» снабжен различными программами поиска, включая программу «поиск объекта заданного типа», способен запоминать визуальные образы объектов, имеет автоматическую настройку и схему подавления влияния минерализации грунта.

Дальность обнаружения пистолета Макарова — 70 см, колодезного люка — 150 см, монеты диаметром 25 мм — 35 см.

Малогабаритный «Сфинкс ВМ-311» и портативный «Сфинкс ВМ-611» (рис. 2.66) имеют ступенчатую регулировку чувствительности. Автоматический селективный грунтовой металлодетектор «Сфинкс ВМ-911» снабжен световой и звуковой индикацией.

Дальность обнаружения монеты диаметром 25 мм — примерно 30 см, пистолета Макарова — 50 см, колодезного люка — 180 см. Масса 0,99 кг.

Сравнительные характеристики отечественных металлодетекторов АКА-7202, АКА-7210, АКА-7215, «Сфинкс ВМ-311», «Сфинкс ВМ-611» приведены в табл. 2.1.

Последними разработками в области металлодетекции явилась разработка селективных металлодетекторов.

Селективный импульсный металлодетектор СИМ-13 (рис. 2.67)

Таблица 2.1

Характеристики отечественных металлодетекторов

Характеристика	АКА-7202	АКА-7210	АКА-7215	«Сфинкс ВМ-311»	«Сфинкс ВМ-611»
Дальность обнаружения пистолета Макарова, см	30	35	35	15	25
Дальность обнаружения диска из цветного металла Ø25 мм, см	13	17	17	6	15
Распознавание цветных и черных металлов	Нет	Есть	Есть	Нет	Нет
Вид индикации	Звуковая, световая	Звуковая, световая	Звуковая, световая	Звуковая	Звуковая, световая
Регулировка чувствительности	Плавная	Нет	Плавная	Ступенчатая	–
Конструктивное исполнение	Портативное	Малогабаритное	Портативное	Малогабаритное	Портативное
Габариты, мм	400×145×35	165×82×32	400×145×35	190×70×30	410×80×30
Масса, кг	0,35	0,26	0,35	0,2	0,3

Рис. 2.67. Селективный импульсный металлодетектор СИМ-13

предназначен для обнаружения металлических неоднородностей в однородных, в том числе в металлосодержащих средах. Металлодетектор позволяет обнаружить металлические предметы в однородной среде, которая содержит отдельные однотипные металлические включения, например крепежные и другие изделия — болты, шурупы, кронштейны, уголки, розетки, выключатели. Условием обнаружения является то, что находящийся вблизи данных изделий или непосредственно в них или за ними металлический предмет более чем на 20 % изменяет хотя бы один из их параметров, например эквивалентные размеры или глубину размещения.

СИМ-13 выявляет такие неоднородности, как металлические тонкостенные корпуса малогабаритных электронных блоков, заделанных в строительных конструкциях с регулярным армированием, например

полу, потолке, стенах. Металлодетектор СИМ-13 позволяет оператору оценить форму, расстояние до обнаруженного объекта, его поперечные размеры и толщину. Варианты исполнения:

- блок с управлением на основе Touch Screen (без кнопок);
- блок с возможностью подключения любых внешних устройств с помощью технологии Wi-Fi (802.11n 2,4 ГГц) для управления и получения данных с устройства.

Основные характеристики металлодетектора: расстояние обнаружения/идентификации металлического предмета типа батарея «Крона» при работе в режиме максимальной мощности не менее 20/15 см; расстояние обнаружения/идентификации металлического предмета типа батарея «Крона» на фоне металлического профиля (алюминиевый уголок) не менее 15/10 см; чувствительность приемника (при соотношении сигнал/шум не менее 10 дБ) не ниже 1 мкВ; время анализа в одной пространственной точке, не более 0,2 с; динамический диапазон приемника не менее 120 дБ.

Звуковая индикация обнаружения осуществляется на головные телефоны. Графическая индикация обнаружения на 4,3" TFT дисплее. Время автономной работы не менее 6 часов.

2.7.2. Приборы рентгеновизуального контроля

Рентгеновское излучение представляет собой электромагнитное излучение, состоящее из незаряженных частиц — фотонов. Для целей контроля целесообразно использовать только «тормозное» излучение, возникающее в рентгеновской трубке при ударе о мишень свободных электронов, ускоренных до высоких энергий. Рентгеновские методы контроля базируются на регистрации тормозного излучения, которое, испытывая в зависимости от распределения плотности материалов различное ослабление, несет информацию о внутреннем строении, т. е. образует рентгеновское изображение объекта, которое затем преобразуется в оптическое.

Принципиальная схема рентгеновизуальной установки приведена на рис. 2.68. Излучение от рентгеновской трубки *1* проходит через объект *2* и преобразователем *3* трансформируется в световой, электронный или потенциальный рельефы, соответствующие рентгеновскому изображению объекта. Полученный рельеф можно воспринимать непосредственно, если он световой, или через систему электронно-оптического усиления и вторичного преобразования *4*, переводящую его в изображение на выходном экране *5*.

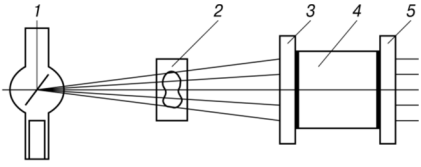


Рис. 2.68. Принципиальная схема рентгеновизуальной установки

Рентгеновская трубка — электровакуумный высоковольтный прибор, предназначенный для генерирования рентгеновского излучения посредством бомбардировки анода (мишени) пучком электронов, ускоренных приложенным к электродам трубки напряжением. Простейшая рентгеновская трубка представляет собой запаянный стеклянный или керамический баллон с разряжением $10^{-6} \ldots 5 \cdot 10^{-7}$ мм рт. ст., внутри которого расположены на фиксированном расстоянии друг от друга катодный и анодный узлы.

Существуют трубки непрерывного и импульсного излучения. Достоинством последних является малая энергоемкость и меньшее облучение оператора за счет малого времени экспозиции (формирования изображения в процессе облучения).

По способу преобразования различают:

- люминесцентные устройства, в которых используются свойства люминофоров преобразовывать некоторую долю поглощаемой энергии рентгеновского излучения в свет;
- электронные, преобразующие рентгеновское изображение в электронное, которое затем трансформируется люминесцентным или рентгенографическим преобразователем в видимое;
- рентгенографические пленки, в которых рентгеновское изображение преобразуется в оптическое в результате взаимодействия излучения с эмульсией рентгеночувствительного материала;
- полупроводниковые, в которых рельеф проводимости, образующийся на фотопроводящем слое, преобразуется затем в потенциальный рельеф и видимое изображение.

Основное требование, которое предъявляется к преобразователям, — возможность оптимальной трансформации рентгеновского изображения в адекватное, т. е. в оптическое, видеосигнал, потенциальный рельеф и т. д. При этом должна быть обеспечена минимально возможная поглощенная доза излучения просвечиваемым объектом.

Главной задачей повышения ценности видимого изображения является увеличение его яркости. Повышение эффективности рентгенолюминофоров даже до 100 % может привести к увеличению яркости всего в несколько раз. Применение усилителей рентгеновского изображения позволяет увеличить яркость исходного изображения в тысячу раз и более. Усилитель рентгеновского изображения (УРИ) представляет собой преобразователь рентгеновского изображения в видимое с одновременным увеличением яркости. Усиленное по яркости изображение наблюдается оператором с экрана рентгеновского электронно-оптического преобразователя (РЭОП) либо с видеоконтрольного устройства замкнутой телевизионной системы, входящей в состав УРИ.

В простейших комплексах рентгеновского контроля применяют люминофорные преобразователи, трансформирующие рентгеновское изображение непосредственно в видимое.

В рентгенотелевизионных комплексах рентгеновское изображение объекта сначала преобразуется входным экраном в видимое. Затем видимое изображение проецируется при помощи светосильной оптики на матрицу передающей телевизионной трубки. В трубке изображение преобразуется в видеосигнал, который после обработки в телевизионном блоке снова трансформируется в видимое на экране видеоконтрольного устройства. В качестве передающих телевизионных трубок применяют в основном видиконы и изоконы.

При проведении поисковых мероприятий широко применяются мобильные рентгенотелевизионные комплексы.

Переносные рентгенотелевизионные установки. Для обеспечения защиты информации в настоящее время существует большой арсенал специальных технических средств, в основе которых положены методы радиационного неразрушающего контроля. От стационарных установок, оборудованных полной биологической защитой, до малогабаритных переносных, которые укладываются в одну относительно небольшую упаковку. С их помощью можно осуществлять обследование и небольших подарков и различных несущих строительных конструкций из железобетона или кирпича.

Малогабаритные переносные рентгенотелевизионные установки предназначены для проведения радиоскопического контроля предметов интерьера, багажа, почтовых отправлений и различных бытовых предметов в стационарных и полевых условиях. С помощью установок могут быть обнаружены инородные включения, отличающиеся по плотности от окружающего их материала контролируемого объекта, независимо от предназначения этих включений. То есть можно обнаружить и систему передачи информации, и взрывное устройство. К достоинствам малогабаритных установок можно отнести следующее:

- быстрое развертывание на месте проведения поиска;
- хорошая оперативность в работе;
- высокая производительность;
- возможность записи теневых изображений в электронную память интроскопа или персонального компьютера для последующего анализа и обработки;
- возможность работы от аккумуляторов.

В состав установок входят рентгеновский аппарат и рентгенотелевизионный интроскоп, которые функционально связаны между собой.

Для осуществления контроля к объекту вплотную придвигается блок преобразователя интроскопа, а излучатель рентгеновского аппа-

рата размещается с противоположной стороны на некотором расстоянии от объекта.

При включении установки поток рентгеновского излучения проходит через контролируемый объект, ослабляется в зависимости от свойств материалов его фрагментов. В результате из контролируемого объекта выходит уже неравномерный поток, интенсивность которого в разных точках его сечения будет отражать внутреннее строение контролируемого объекта. Возникает радиационное теневое изображение. Преобразователь интроскопа светится в зависимости от интенсивности падающего на него потока рентгеновского излучения. Таким образом, радиационное изображение преобразуется в видимое. Это изображение считывается телевизионной камерой и передается по кабелю в блок управления и индикации.

В переносных установках используются малогабаритные моноблочные рентгеновские аппараты. Это аппараты непрерывного действия с анодным током до 5 мА и максимальным анодным напряжением до 90 кВ, импульсные аппараты с напряжением до 250 кВ и микрофокусные аппараты с анодным током до 0,1 мА и с напряжением до 150 кВ. Выбор рентгеновского аппарата влияет на предельную доступную для контроля толщину объекта и на качество получаемого изображения. Наиболее часто используются микрофокусные рентгеновские аппараты. По сравнению с сильноточными и импульсными аппаратами они позволяют получать увеличенное до 12 раз изображение отдельных фрагментов контролируемого объекта и оказывают наименьшее радиационное воздействие на окружающих вследствие небольшого анодного тока.

Рентгенотелевизионная установка «Премьер» (рис. 2.69) с микрофокусным излучателем РИ-100М позволяет осуществлять контроль объектов, имеющих эквивалентную по алюминию толщину до 40 мм. В настоящее время установка снята с производства. Размер рабочего поля преобразователя 290×390 мм.

Размер экрана монитора по диагонали 30 см. Чувствительность контроля соответствует выявлению медной проволоки диаметром 0,2 мм без преграды или 0,4 мм за преградой из алюминия толщиной 10 мм. Время включения излучателя для получения изображения 8 с. Количество записываемых в долгосрочную память изображений 3000.

Теневое изображение контролируемого объекта может быть представлено в позитивном, негативном и дополнительно проконтрастированном виде. Общая масса установки 40 кг. Электропитание осуществляется от сети переменного тока частотой 50 Гц и напряжением 220 В.

Переносные рентгенотелевизионные установки серии «Норка» (рис. 2.70) создавались по модульному принципу построения. В сос-

Рис. 2.69. Рентгенотелевизионный комплекс «Премьер»

Рис. 2.70. Малогабаритная рентгенотелевизионная установка «Норка»

тав установки могут входить как микрофокусные излучатели, так и сильноточные серии РАП. Установки комплектуются одним из блоков управления: БУ-4М или БУ-5. Миниатюрный пульт БУ-4М снабжен монитором размером 12" и памятью на 30000 изображений, которые, при желании, могут быть переписаны в персональный компьютер. В портативном компьютерном блоке управления БУ-5 (монитор размером 15" и памятью на 30000 изображений) реализована возможность цифрового увеличения любого участка изображения. Программное обеспечение позволяет получать псевдоцветные изображения, проводить цифровое улучшение изображений, архивирование рентгентелевизионных изображений, представлять изображения в негативе и позитиве, вносить речевые комментарии.

С рентгеновским излучателем РИ-100М «Норка» позволяет осуществлять контроль объектов, имеющих эквивалентную по стали толщину до 40 мм. Размеры рабочего поля трех преобразователей, которые входят в комплект установки, 114×152 мм, 290×390 мм и 410×545 мм. Размер экрана монитора по диагонали 15 см. Чувствительность контроля соответствует выявлению медной проволоки

Рис. 2.71. Рентгенотелевизионный комплекс Flat Scan 27

диаметром 0,03 мм без преграды. Время включения излучателя для получения изображения 8 с. Количество записываемых в долгосрочную память изображений 128. Общая масса установки 19 кг. Электропитание осуществляется от сети переменного тока частотой 50 Гц и напряжением 220 В или от аккумуляторного блока. Установка комплектуется блоком телекамеры, который устанавливается на один из трех сменных преобразователей. Выбор конкретного преобразователя обусловливается габаритами контролируемого объекта и требуемым пространственным разрешением. В комплект поставки могут входить один, два либо несколько преобразователей.

Рентгеновские аппараты являются источниками ионизирующего излучения, и при работе с ними необходимо строго выполнять требования по радиационной безопасности, содержащиеся в эксплуатационной документации.

Переносной рентгенотелевизионный комплекс Flat Scan 27 (рис. 2.71) предназначен для быстрого, радиационно-безопасного рентгеновского обследования внутреннего содержимого различных предметов, багажа, грузов, посылок, транспортных средств с целью обнаружения оружия, наркотиков, взрывных устройстви других запрещенных предметов; поиска скрытых систем съема аудио- и видеоинформации в помещениях (стены, мебель, орг. техника, средства связи). Может быть использован для дефектоскопии и решения задач техногенной безопасности в полевых условиях. Рентгеновский аппарат работает от встроенной аккумуляторной батареи. Управление напряжением и током через портативный компьютер. Комплекс снабжен тонким плоским рентгенооптическим преобразователем (50 мм в толщину),

способным сканировать предметы, находящиеся в труднодоступных местах; обеспечивает высокое качество передачи изображения; обладает высокой способностьюпроникновения (вплоть до 30 мм стали на 120 кВ, 1 мА); обладает возможностью сканирования на разных скоростях; прост и удобен в использовании.

Переносной рентгенотелевизионный комплекс Flat Scan 27 снабжен тонким рентгенооптическим преобразователем (50 мм в толщину), способным сканировать предметы, находящиеся в труднодоступных местах. Преобразователь обладает высокой чувствительностью, разрешением до 800 микрон (200 микрон детектора в опции); имеет возможность сканировать объекты с различной скоростью, что обеспечивает высокое качество изображения с проникающую способность (вплоть до 30 мм стали на 120 кВ, 1 мА).

Рентгеновские аппараты CP120 и CP160 являются портативными генераторами рентгеновских лучей, работающих на 36 В аккумуляторных батареях. Аппараты генерируют стабильное излучение. Малый размер фокусного пятна обеспечивает возможность геометрического увеличения изображения в 5 раз без потери чёткости. Благодаря возможности регулирования напряжения и тока характеристики рентгеновского излучения могут быть адаптированы к каждому подозрительному объекту контроля. Широкий угол излучения позволяет поместить генератор рядом с рентгенооптическим преобразователем и таким образом увеличить проникающую способность системы. Оператор может выбрать все следующие стандартные операции процессов: реверсировать чёрный и белый цвета, включить псевдоцвет, увеличить изображение, изменить контраст, изменять параметры CP120 и CP160 для обеспечения максимально глубокого проникновения.

Благодаря особой конструкции рентгеновских аппаратов CP120 и CP160 реализована опциональная программа идентификации материалов на основе алгоритма двойной энергии (рис. 2.72). Эта программа обеспечивает выделение различными цветами на рентгенооптическом изображении, представленном на экране портативного компьютера, органические (например, взрывчатку и наркотики) и неорганические

Рис. 2.72. Вид изображений на экране монитора

Рис. 2.73. Подповерхностный локатор «Раскан-4»

(металлы) субстанции, находящиеся в подозрительных предметах багажа.

Рентгеновские аппараты являются источниками ионизирующего излучения, и при работе с ними необходимо строго выполнять требования по радиационной безопасности, содержащиеся в эксплуатационной документации. Кроме того, существенным недостатком при работе с рентгеновской аппаратурой является необходимость подхода к проверяемому объекту с двух сторон. С одной стороны должен находиться излучатель, а с другой — экран, на который фокусируется изображение объекта контроля.

В последнее время появился ряд приборов свободных от этого недостатка. К таким приборам относятся **приборы подповерхностной локации серии «Раскан»**.

Подповерхностный локатор «Раскан-4» (рис. 2.73) предназначен для обследования ограждающих конструкций, а также предметов мебели на наличие скрытно установленных устройств съема и передачи информации. Максимальная глубина зондирования 0,2 м; разрешение в плоскости зондирования 2 см; мощность генератора 10 мВт; количество рабочих частот 5; число поляризаций принимаемого сигнала 2; число одновременно получаемых радиоизображений 10. «Раскан-4» представляет собой многочастотный голографический радиолокатор, работающий на отражение, т. е. передающая и приемная части антенны расположены с одной стороны зондируемой поверхности, поэтому не требуется иметь двухсторонний доступ к исследуемому объекту. Отражение электромагнитного излучения происходит от объектов, обладающих контрастом диэлектрической проницаемости по отношению к среде, в которой они находятся. В силу этого на получаемых изображениях видны не только металлические объекты, но и диэлектрические неоднородности, например пустоты, что отличает данный прибор от широко используемых в настоящее время металлоискателей.

Рис. 2.74. Подповерхностный радиолокатор «Раскан-4/2000»

Подповерхностный радиолокатор «Раскан-4/2000» (рис. 2.74) с частотой зондирования 2 ГГц предназначен для зондирования строительных конструкций с целью выявления подслушивающих устройств.

«Раскан-4/2000» позволяет проводить одностороннее зондирование, а не на просвет, как в рентгенотелевизионной технике, имеет полностью цифровое управление и ЖК индикатор. Частота зондирования 2 ГГц. Прибор имеет увеличенную глубину зондирования. Антенна радиолокатора снабжена маршрутными колесами, что облегчает работу при обследовании больших площадей. Возможность подключения к ПЭВМ (USB-порт), программное обеспечение в комплекте. Прибор обеспечивает возможность выделения объектов расположенных как на фоне другого объекта, так и за ним (например, небольшой объект, расположенный за протяжённой арматурой); способность обнаруживать не только металлические объекты, но и диэлектрические неоднородности. Частотный диапазон 1,6...2,0 ГГц; 5 рабочих частот; выходная мощность $6 \cdot 10^{-3}$ Вт.

2.7.3. Тепловизионные приборы

При размещении любого объекта в укрывающей среде неизбежно проявляются нарушения ее структуры (прежде всего плотности) даже при самом тщательном маскировании. В результате возникает различие в степени теплового излучения маскирующего слоя, расположенного над объектом, и естественного фона. Уровень излучения зависит от материала, температуры, влажности, состояния поверхности маскирующего слоя и ряда других факторов.

Тепловизионные приборы применяют для обнаружения средств съема информации, установленных в ограждающих конструкциях помещений, а также для определения параметров и времени появления тепловых следов, т. е. создания термографических изображений. В первых тепловизионных приборах для повышения чувствительности использовалось охлаждение жидким азотом, что делало небезопасным их практическое применение, хотя существенно улучшало чувствительность приборов. Представителем этого класса является тепловизионный комплекс IRTIS-2000.

Тепловизионный комплекс IRTIS-2000 (рис. 2.75) в диапазоне температур от -20 до $+200$ °C имеет чувствительность от 0,05 до 0,35 °C. Сканирование кадра с разрешением 256×256 строк занимает не более 1,5 с. Габаритные размеры инфракрасной камеры (ИК)

Рис. 2.75. Тепловизионный комплекс IRTIS-2000

200×140×100 мм при массе около 2,5 кг. Потребление энергии до 1,5 Вт позволяет обеспечить непрерывное время работы от 6 В NiCd аккумуляторов не менее 5 ч.

Тепловизор ИРТИС-2000 предназначен для осмотра объектов в инфракрасном диапазоне спектра («тепловая картинка»), измерения температуры в любой их точке, наблюдения динамики тепловых процессов, а также создания банка данных теплового состояния по каждому из наблюдаемых объектов. Принцип работы IRTIS-2000 основан на сканировании температурного излучения в поле зрения камеры оптико-механическим сканером с одноэлементным высокочувствительным ИК-приемником и трансформации этого излучения в электрический сигнал аналого-цифровым преобразователем.

Камера содержит зеркально-линзовую оптику с малым количеством отражающих поверхностей, что уменьшает потери оптической системы и упрощает ее настройку. Ряд примененных в конструкции ноу-хау в сочетании с новейшими компьютерными технологиями позволяет достичь высокой повторяемости геометрии последовательных кадров и равномерной чувствительности по всему полю кадра. Применение особых методов сканирования, таких как суммирование кадров и усреднение, позволяет повысить чувствительность прибора до 0,02 °С. Инфракрасная камера прибора представляет собой механический сканер с одноэлементным ИК приемником. Малое количество преломляющих и отражающих поверхностей зеркально-линзовой оптической системы обеспечивает минимальные потери и простоту настройки оптического тракта, что позволяет достичь равномерной чувствительности по полю кадров и высокой повторяемости их геометрии.

Рис. 2.76. Профессиональный тепловизор Flir серии P

Инфракрасный приемник тепловизионного прибора может комплектоваться системой термоэлектрического охлаждения или системой охлаждения жидким азотом. Базовая модель камеры, укомплектованная последней системой, имеет чувствительность не менее 0,05 °С. Наличие компьютера позволяет производить обработку информации непосредственно в процессе сканирования термограмм.

В настоящее время все большее применение находят неохлаждаемые тепловизоры. Одним из представителей этой группы приборов является переносной неохлаждаемый тепловизор ТН-3 («Спектр»). Он имеет встроенный цифровой процессор, что обеспечивает возможность наблюдения на экране изображений в ИК диапазоне (8...13 мкм) объекта при минимальной разности температуры элементов его поверхности 0,15 °С. Позволяет осуществить дистанционное измерение температур в выбранной зоне в интервале от −40 до + 600 °С. В комплект тепловизора входит камера размером 110×165×455 мм и массой 6 кг, малогабаритный монитор и блок питания. «Спектр» позволяет получать видимое и ИК изображение с записью в блок памяти, имеет связь с ПЭВМ, с помощью которой происходит обработка тепловизионных изображений с помощью специального программного обеспечения. Рабочий спектральный диапазон 8... 13 мкм. Геометрическая разрешающая способность 160×120 пикселей. Штатные ИК объективы с фокусным расстоянием 9 или 25.

Профессиональный тепловизор Flir серии P (рис. 2.76) — тепловизор высшего уровня. Все новейшие разработки и возможности внесены в данную серию приборов. Высокое разрешение 640×480 пикселей, чувствительность 30 мК и даже модуль GPS в версии 660 — вот неполный список приемуществ данных тепловизоров. Тепловизоры этих серий также имеют функцию Bluetooth для записи речевых комментариев и беспроводной связи с Extech MO297 (измеритель влажности) и Extech EX845 (токоизмерительные клещи) — функция MeterLink.

Рис. 2.77. Профессиональный тепловизор NEC TH9260

Профессиональный тепловизор NEC TH9260 (рис. 2.77). В основу тепловизора вошла новая лицензионная матрица японского производства размерностью 640×480 элементов. Встроенная видеокамера высокого разрешения позволяет получить композитное изображение (наложение термограммы на видимую картинку).

Встроенный лазерный целеуказатель позволяет точно локализовать место нагрева. Тепловизор имеет возможность подсветки объекта контроля при низкой освещенности. Диапазон измерения температуры от −40 °C до + 500 °C (опционально до + 2000 °C). Температурное разрешение 0,02 °C. Погрешность измерения температуры ±2 °C или ±2 % от измеряемой величины. Спектральный диапазон 8...14 мкм. Тип детектора — неохлаждаемая микроболометрическая матрица 640×480 элементов. Оптическое поле зрения стандартное 21,7°×16,4°. Мгновенный угол обзора 0,6 мрад. Диапазон фокусировки от 30 см до бесконечности. Частота кадров 30 Гц. Временной интервал измерений. Запись последовательности на внутреннюю память (мах. 6656 кадров при 30 Гц) или карту памяти. Предусмотрена регистрация событий. Повышение соотношения сигнал/шум. Суммирование 2, 8,..., 64 и пространственный фильтр (Вкл./Выкл.). Динамический диапазон 16 битов. Коэффициент коррекции по излучательной способностиот 0,10 до 1,00 с шагом 0,01. Предусмотрена компенсация фона. Визуализация: дисплей 5,6", LCD видоискатель. Предусмотрены функции автоматической регулировки: автофокус; авто (уровень/чувствительность/фокус); автоматическая настройка уровня. Автоматическая настройка чувствительности. Функции анализа предусматривают индикацию температуры и коэффициента излучения в нескольких точках (мах. 10). Отображение дельты температур.

Индикация max/min температур с фиксацией (по всему снимку или по области). Функция сигнализации по области или по всему экрану. Цифровое увеличение ×2, ×4, ×6, ×8. Видеовыход NTSC/PAL, S-видео. Интерфейс USB 2.0, RS-232C, IEEE 1394 FireWire. Хранение данных. Карта памяти CF, форматы: SIX, BMP, JPG, MPEG.

2.7.4. Эндоскопы

Для визуального контроля труднодоступных зон, характеризуемых минимальными размерами входных отверстий, сложными профилями и плохой освещенностью, предназначены волоконно-оптические приборы — эндоскопы.

В состав прибора (рис. 2.78) входят мощный источник света *1*, световод освещения *2*, световод изображения *3* с объективом *4*, окуляр *5* с регулятором резкости *6*, манипулятор *7* гибкого участка объединенной (рабочей) части световодов *8*.

В качестве источника света используется галогенная лампа, снабженная отражателем с интерференционным покрытием. Лампа и торцевая часть световода освещения охлаждаются воздушным потоком, создаваемым вентилятором. По световоду освещения свет передается в труднодоступную зону. Изображение, увеличенное объективом, передается по световоду наблюдателю. Качество изображения устанавливается регулятором резкости. Различают жесткие, гибкие, полужесткие эндоскопы.

Жесткие эндоскопы представляют собой прямую металлическую трубку диаметром от 2,7 до 10 мм со специальной линзовой системой. Применяются такие эндоскопы достаточно редко.

В гибких эндоскопах передача изображения осуществляется по оптоволоконному кабелю. Распространение света по оптоволокну сопровождается существенными потерями, поэтому длина рабочей части, как правило, не превышает 1,5 м. Существуют также и эндоскопы длиной порядка 25 м, но в таких изделиях передача изображения осуществляется по радиоканалу и только подсветка идет по оптоволокну. К особенностям гибких эндоскопов относится возможность изгиба дистального конца изделия на ±180°, что позволяет как бы оглядеться по сторонам. В комплект поставки обычно входит устройство

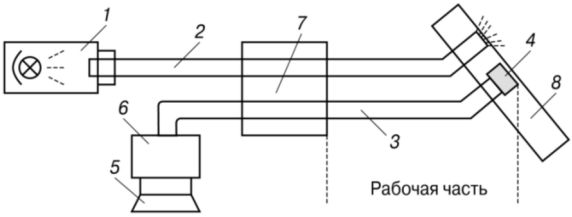


Рис. 2.78. Принципиальная схема эндоскопа

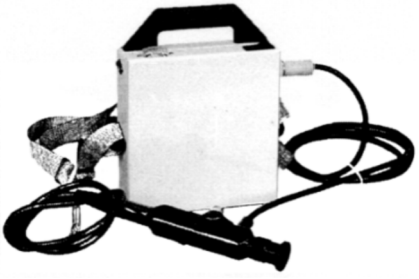


Рис. 2.79. Эндоскоп серии ЭТ-2

Рис. 2.80. Эндоскоп серии ТЭУ

подсветки, обеспечивающее возможность работы в отсутствии освещения. В последнее время стала возможна поставка видеоскопов, т. е. эндоскопов с выводом изображения на монитор.

Полужесткие эндоскопы выполнены на базе оптоволокна в специальной оплетке, которая позволяет сохранять форму после изгиба (иногда такие эндоскопы называют фиброскопами или флексоскопами).

Наиболее широкое распространение в своё время получили эндоскопы серии ЭТ-2 (рис. 2.79).

Полугибкие технические эндоскопы серии ТЭУ (рис. 2.80). Рабочая часть полугибких эндоскопов находится внутри полугибкой металлической трубки из нержавеющей стали — флекстрона. Внешней металлической оболочке рабочей части предварительно может быть задана необходимая геометрическая форма (эффект запоминания заданной формы), что позволяет обследовать «теневые» полости, недоступные для эндоскопов других типов (жестких, гибких). Полугибкие эндоскопы серии ТЭУ имеют управляемый дистальный конец, изгибающийся в одной плоскости. Механизм управления изгибом имеет двухстороннюю артикуляцию и оборудован механизмом фиксации.

В настоящее время для визуального контроля труднодоступных мест разработаны и применяются мобильные телевизионные эндоскопы. Контроль и обнаружение объектов осуществляется с использованием миниатюрных видеокамер и выводом изображения на монитор. Одним из первых представителей этих приборов на российском рынке является мобильный телевизионный эндоскоп «Кобра-ТВ», который представляет собой прибор дистанционного визуального контроля с автономным питанием.

Эндоскоп «Кобра-ТВ» (рис. 2.81) представляет собой сложный телевизионный прибор, построенный на взаимосвязанных системах, объединенных в единый комплекс.

Эндоскоп включает следующие системы:

- корпусную механическую конструкцию и гибкую рабочую часть;

Рис. 2.81. Телевизионный эндоскоп «Кобра-ТВ»

- систему управления изгибаемым концом и рабочей частью эндоскопа;
- телевизионную систему наблюдения изображения, его регистрации и ввода в компьютер для обработки и анализа;
- осветительную систему;
- систему электрического питания;
- механическую оснастку для крепления эндоскопа, продвижения и позиционирования его рабочей части.

Прибор имеет следующие технические характеристики: рабочая часть резиновая термостойкая оболочка на каркасе из стальной ленты с наружным бронированным стальным покрытием; диаметр гибкой рабочей части 13,5 мм; длина гибкой рабочей части 1000...2700 мм; диаметр миниатюрной телевизионной камеры 27 мм; изгиб конца гибкой рабочей части в горизонтальной плоскости $\pm 90°$; поворот гибкой рабочей части с изгибаемым концом вокруг своей оси от $\pm$ 90° (в сочетании с изгибом конца обеспечивает круговой обзор); миниатюрная аналоговая телевизионная камера, совмещенная с осветителем на основе 8 сверх ярких светодиодов, крепится при помощи разъема на изгибаемом конце; диагональ экрана видеомонитора (видеоплейера) 12,5 см (9,5 см); угол обзора объектива 50°; предельная дальность наблюдения при собственном освещении до 200 см; предельное разрешение на расстоянии 5 мм, 10 см, 20 см от объектива 10 мкм, 40 мкм, 200 мкм соответственно; питание осветителя 12 В от внешней аккумуляторной батареи.

Современные мобильные телевизионные эндоскопы по своим параметрам приблизились к оптоволоконным эндоскопам, однако моде-

Рис. 2.82. Эндоскоп ЭТВЦ

Рис. 2.83. Эндоскоп ЭТВЦ-Д

ли ценовой доступности не имеют возможности управления дистальным концом для кругового обзора места поиска. Модели, позволяющие осуществить круговой обзор места поиска и имеющие высокую разрешающую способность, по своему ценовому диапазону существенно превосходят оптиковолоконные эндоскопы.

Эндоскоп ЭТВЦ (рис. 2.82) предназначен для визуального контроля неосвещенных мест внутренних полостей, отверстий, труб и другого труднодоступного пространства с применением телевизионного канала регистрации, изображения. В дистальный конец рабочей части эндоскопа встроена миниатюрная чёрно-белая или цветная видеокамера. Для подсветки наблюдаемых объектов используется гибкий оптоволоконный жгут. Источник подсветки, изготовленный на основе сверхяркого светодиодного излучателя мощностью 3 Вт, расположен в корпусе эндоскопа. Изображение выводится на съёмный ЖК монитор. Питание прибора осуществляется от 12 В сетевого адаптера. Для регистрации и заполнения изображений возможно подключение внешнего видеорегистратора.

Эндоскоп ЭТВЦ-Д. Основное назначение телевизионного эндоскопа ЭТВЦ-Д (рис. 2.83) — визуальный контроль замкнутых внутренних полостей различных объектов, к которым затруднен доступ. Эндоскоп является моноблочной конструкцией, т. е. при работе не требуется ни внешний источник питания, ни внешний осветительный блок, традиционно используемые в приборах подобного типа. Источником питания служат 4 батареи типа АА, также возможна работа прибора от внешнего адаптера 12 В.

Источником света являются несколько минисветодиодов, расположенных в рабочей части эндоскопа рядом с видеокамерой. Вывод изображения с видеокамеры производится на микровидеодисплей, который также расположен в корпусе прибора. Такие технические решения позволили существенно уменьшить габариты эндоскопа и упростить работу с прибором. В эндоскопе предусмотрена возможность

регулировка яркости свечения светодиодов. Может быть установлена цветная или черно-белая камера. Возможен вывод изображения на внешний монитор или видеорегистратор.

2.7.5. Средства радиационного контроля

Обнаружение подозрительных объектов с радиоактивными свойствами осуществляется радиометрическими приборами, реагирующими на гамма- или жесткое бета-излучение. В состав радиометра входят:

- детектор ионизирующего излучения в виде газонаполненного счетчика Гейгера–Мюллера или пропорционального счетчика, включающего в себя сцинтиллятор, фотоэлектронный умножитель, ионизационную камеру, кристалл полупроводник;
- счетчик импульсов или усилитель выходного тока детектора;
- цифровой или стрелочный индикатор;
- устройство питания.

Заряженная частица (гамма-квант), попадая в зону действия детектора, вызывает ионизацию рабочего вещества. Образующиеся заряды собираются на электродах детектора, формируя импульс тока. Количество импульсов за некоторое фиксированное время подсчитывается, а результат отображается на индикаторе. Время измерения для сцинтилляционного детектора 1...2 с, для радиометров со счетчиками Гейгера-Мюллера — от 20 до 50 с.

Величина, которую измеряют радиометры, называется мощностью экспозиционной дозы (МЭД) гамма-излучения. Для ее оценки чаще всего используют внесистемные единицы (рентген): Р/ч, Р/мин, Р/с, мР/мин, мР/с, мкР/ч, мкР/мин, мкР/с. Фоновая МЭД должна составлять от 5 до 30 мкР/ч. Если МЭД, создаваемая объектом, в несколько раз превышает фоновую, его можно считать подозрительным.

Основной дозиметрической величиной является эквивалентная доза, являющаяся мерой потери энергии излучения в единице массы биологической ткани. Единица измерения в системе СИ — зиверт (Зв), внесистемная — бэр (1 бэр = 10^{-2} Зв). Поглощенная тканевая доза, измеренная в бэрах, примерно равна экспозиционной дозе, измеренной в рентгенах.

При работе с источниками ионизирующего излучения, чтобы не допустить заметного вредного воздействия излучения на организм человека, необходимо руководствоваться Нормами радиационной безопасности НРБ-99/2009, утвержденными постановлением Главного государственного санитарного врача Российской Федерации от 7 июля 2009 года № 47. В этих нормах установлены основные пределы доз облучения для следующих категорий облучаемых лиц: для персонала

(группы А и Б) и для всего населения. Под персоналом понимаются лица, работающие с техногенными источниками излучения (группа А) или находящиеся по условиям работы в сфере их воздействия (группа Б).

Для персонала группы А установлена эффективная доза 20 мЗв в год в среднем за любые последовательные 5 лет, но не более 50 мЗв в год. Для персонала группы Б основные пределы доз равны 1/4 значений для персонала группы А. Для населения установлена эффективная доза 1 мЗв в год в среднем за любые последовательные 5 лет, но не более 5 мЗв в год.

В целях выявления источников ионизирующего излучения используются различные виды дозиметров. Наиболее простые показывают факт наличия ионизирующих излучений, превышающих установленный порог. Более сложные позволяют измерять (оценивать) мощность дозы гамма-излучений, измерять плотность потока бета-излучений от загрязненных поверхностей, а также производить поиск источников ионизирующих излучений.

Рис. 2.84. Цифровой сигнализатор ионизирующих излучений «Штуф-М1»

Цифровой сигнализатор ионизирующих излучений «Штуф-М1» (рис. 2.84) предназначен для измерения мощности экспозиционной дозы гамма-излучения, а также для оценки плотности потока альфа-, бета-излучения от загрязненных поверхностей и загрязненности альфа-, бета- и гамма-излучающими нуклидами проб почвы, воды, пищи и т. п. Прибор имеет следующие характеристики: диапазон энергий рентгеновского и гамма излучений от 20 кэВ до 3000 кэВ; бета-излучения до 5500 кэВ; основная погрешность измерения по гамма-излучению ± 30 %; время готовности к работе после включения не более 20 с; время непрерывной работы от батареи типа «Корунд» напряжением 9 В не менее 30 ч; диапазон рабочих температур от 0 °С до 45 °С; габаритные размеры $140 \times 65 \times 30$ мм; масса 0,3 кг.

Дозиметр цифровой ДКГ-АТ-2503 (рис. 2.85) позволяет осуществить индивидуальный дозиметрический контроль и проводить измерение МЭД и ЭД гамма-излучения.

Учет собственного фона и микропроцессорная обработка обеспечивают высокую точность измерения дозы в широком (6,5 порядков) диапазоне мощностей доз. Управление режимами работы, выполнение вычислений, вывод информации на ЖК индикатор с подсветкой,

Рис. 2.85. Цифровой дозиметр ДКГ-АТ-2503

Рис. 2.86. Дозиметр поисковый микропроцессорный PM-1401

самодиагностика выполняются микропроцессором. Наличие энергонезависимой памяти позволяет запомнить и сохранить при отключенном питании накопленную дозу, историю накопления дозы. Калибровка дозиметра в процессе производства осуществляется на водном фантоме 30×30×15 см. Дозиметр размещается в нагрудном кармане одежды. Программное обеспечение для считывания и учета показаний позволяет осуществлять:

- считывание/установку индивидуального и заводского номеров дозиметра;
- изменение порогов по дозе и мощности дозы;
- запрет/разрешение выбора порогов по дозе и мощности дозы от кнопки на передней панели дозиметра;
- изменение интервала накопления доз от 1 до 255 мин и возможность определения накопленной дозы за любой интервал времени в течение рабочей смены;
- автоматическую запись в память не менее 800 значений дозы, накопленной за выбранный интервал накопления;
- сброс (обнуление) накопленной дозы;
- запрет/разрешение сброса накопленной дозы от кнопки на передней панели дозиметра;
- автоматическую запись информации в базу данных, документирование.

Дозиметр поисковый микропроцессорный PM-1401 (рис. 2.86) — высокочувствительный поисковый дозиметр, предназначенный для обнаружения и локализации источников гамма-излучения в полевых условиях и измерения мощности эквивалентной дозы гамма излучения; обладает повышенной чувствительностью к оружейным материалам. Прибор прочен к падению с высоты 0,7 м на бетонный пол, устойчив к воздействию соляного тумана и обладает небольшим энергопотреблением (время непрерывной работы от одного комплекта батарей

1000 ч). Специальный алгоритм, реализованный в приборе, позволяет осуществлять поиск и локализацию даже слабых источников в полях радиоактивного излучения, создаваемых более интенсивными источниками.

После включения прибор автоматически осуществляет самодиагностику, затем измеряет фон, рассчитывает порог в зависимости от уровня фона и установленного коэффициента, затем переходит в режим поиска. В случае, если излучение от источника превышает порог, происходит срабатывание звукового или вибрационного сигнализатора, при этом частота следования сигналов увеличивается по мере приближения к радиоактивному источнику.

Контрольные вопросы для самостоятельной работы

1. Влияние внешних помех на работу индикаторов поля, частотомеров.
2. Какие трудности могут возникнуть при первичной проверке помещения индикатором поля?
3. Принципы построения индикаторов поля.
4. Сервисные возможности различных моделей индикаторов поля.
5. От каких факторов зависит дальность обнаружения радиомикрофонов при использовании индикаторов поля?
6. Возможно ли использование радиочастотомеров в качестве индикаторов поля?
7. Основные характеристики радиоприемных устройств.
8. Какими характеристиками следует руководствоваться при выборе конкретной модели сканирующего приемника?
9. Что такое радиоприемные устройства ближней зоны и каковы их отличия от сканирующих приемников?
10. Какие виды устройств несанкционированного съема информации можно выявить при использовании:

а) сканирующих приемников;

б) приемников ближней зоны.

11. Принципиальные отличия и назначение сканирующих приемников и измерительных приборов (селективные микровольтметры, анализаторы спектра).
12. С помощью какой радиоприемной аппаратуры можно выявить наличие устройств несанкционированного съема информации:

- с дистанционным управлением;
- со скачкообразным изменением частоты;
- с широкополосным спектром.

13. Можно ли, используя радиоприемное устройство, работающее в режиме WFM, распознать сигналы с AM?
14. Принципы и алгоритмы идентификации сигналов устройств несанкционированного съема информации применяемые в автоматизированных комплексах.
15. Назначение этапа адаптации автоматизированных комплексов к окружающей электромагнитной обстановке.
16. Факторы, влияющие на точность определения местоположения устройств несанкционированного съема информации методом акустической локации.
17. Сравнение характеристик специализированных аппаратно-программных комплексов и комплексов на базе СПО.
18. Критерии применения многоканальных поисковых комплексов.

19. Достоинства и недостатки различных методов обнаружения сигналов устройств несанкционированного съема информации, используемых в многоканальных комплексах.

20. Причины появления откликов при механическом соприкосновении двух металлов.

21. Может ли влиять работа радиотелефонов на работу локаторов и наоборот?

22. Какие трудности могут возникнуть при обнаружении экранированных закладок и почему?

23. Достоинства и недостатки импульсного и непрерывного режимов работы нелинейных локаторов.

24. Причины возникновения «хруста» при обнаружении коррозионных полупроводников.

25. Возможно ли разрушение коррозионного диода при облучении мощным импульсным сигналом?

26. Какие характеристики локаторов влияют на их обнаружительные свойства при поиске в укрывающих средах:

- мощность излучения?
- частота излучения?
- чувствительность приемника?

27. В каких случаях возможно прослушивание радиомикрофонов?

28. В каких случаях обнаружение закладочных устройств с помощью нелинейного локатора невозможно?

29. Принцип работы вихретоковых металлодетекторов.

30. Схема построения рентгеновских аппаратов неразрушающего контроля.

31. Преимущества импульсных рентгеновских аппаратов.

32. Что является источником информации об объекте для тепловизора?

3 ОРГАНИЗАЦИЯ ИНЖЕНЕРНО-ТЕХНИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

В предыдущих главах пособия были рассмотрены как возможные технические каналы утечки информации, так и возможности современных технических средств по выявлению этих естественных или искусственно созданных каналов. Выявление этих каналов не является самоцелью, а служит основой для построения эффективной системы защиты информации от утечки ее по техническим каналам.

3.1. Организационно-методические основы защиты информации

3.1.1. Общие требования к защите информации

Защита информации в новых экономических условиях представляет собой целенаправленную деятельность собственников информации по исключению или существенному ограничению утечки, искажения или уничтожения защищаемых ими сведений. Защита информации должна предусматривать ее сохранность от широкого круга различных угроз, таких как утечка информации, несанкционированные и непреднамеренные воздействия на неё.

Как правило, защите подлежит категорированная или конфиденциальная информация. В зависимости от вида угроз предусматривается и вид защиты:

- от разглашения и несанкционированного доступа;
- от искажения, копирования, блокирования доступа к ней и ее уничтожения;
- от утраты или уничтожения носителя информации или сбоя его функционирования;
- от утраты или уничтожения носителя информации или сбоя его функционирования из-за ошибок пользователя информацией;
- от сбоя технических и программных средств информационных систем или природных явлений или иных нецеленаправленных на изменение информации воздействий.

Защита информации от технических средств разведки представляет собой совокупность организационных и технических мероприятий, проводимых с целью исключения (существенного затруднения)

добывания злоумышленником информации об объекте защиты с помощью технических средств. Защита от этих средств достигается комплексным применением согласованных по цели, месту и времени мер защиты.

Эффективное противодействие обеспечивается только при комплексном использованиитехнических средств и организационно-технических методов в целях защиты охраняемых сведений об объекте, осуществляемых в соответствии с целями и задачами противодействия, этапами жизненного цикла объекта и способами противодействия. При этом к защите информации предъявляется ряд требований.

Защита должна проводиться *своевременно, активно, разнообразно, непрерывно, рационально, комплексно, планово, скрытно*.

Своевременность. Одним из основных требований является своевременность принятия решения на организацию защиты информации. Ускорение процесса выработки решения необходимо, во-первых, для того чтобы своевременно решить возникшие проблемы и не давать им разрастись до такого состояния, когда решение их станет невозможным или бесполезным, во-вторых, для того чтобы подчиненные имели достаточно времени для выполнения поставленных перед ними задач.

Активность противодействия, прежде всего, предусматривает наступательный, активный характер противодействия, основанный на анализе складывающейся обстановки, умении сделать правильные выводы о возможных действиях потенциального противника, позволяющие упредить их и настойчиво осуществлять эффективные меры противодействия.

Разнообразие противодействия направлено на исключение шаблона в организации и проведении мероприятий и подразумевает творческий подход к его организации и осуществлению.

Комплексность предусматривает проведение комплекса мероприятий, направленных на своевременное закрытие всех возможных каналов утечки информации об объекте. Недопустимо применять отдельные технические средства или методы, направленные на защиту только некоторых, из общего числа возможных, каналов утечки информации.

Непрерывность противодействия предусматривает проведение мероприятий по комплексной защите объекта информатизации на всех этапах жизненного цикла разработки и существования специальной продукции или обеспечения производственной деятельности объекта защиты.

Плановость проведения мероприятий предусматривает, прежде всего, предусмотренные заранее, еще на стадии проектирования и

строительства объекта, мероприятия, направленные на защиту информации.

Скрытность проведения мероприятий направлена, прежде всего, на то, чтобы противник не смог принять контрмеры по выключению дистанционно управляемых, активных средств съема информации. Поэтому важно, чтобы мероприятия по противодействию выглядели правдоподобно и отвечали условиям обстановки, выполнялись в соответствии с планами защиты информации объекта. В связи с этим разрабатываются и осуществляются практические меры по легендированию и маскировке мероприятий, направленных на защиту.

Особое внимание при проведении таких мероприятий должно обращаться на выбор замысла защиты информации объекта, замысла противодействия. Замысел защиты — общая идея и основное содержание организационных, технических мероприятий и мер направленных на маскировку, обеспечивающих устранение или ослабление (искажение) демаскирующих признаков и закрытие технических каналов утечки охраняемых сведений.

В основе защиты информации лежит совокупность правовых форм деятельности собственника и организационно-технических мероприятий, реализуемых с целью выполнения требований по сохранению защищаемых сведений и информационных процессов, а также мероприятия по контролю эффективности принятых мер защиты информации.

Рассматривая вопросы организации защиты информации от ее утечки по техническим каналам, необходимо отметить, что защита информации не является отдельными, разовыми эпизодами и мероприятиями, а как указано в требованиях, предъявляемых к защите, она должна вестись комплексно и непрерывно.

Грамотное построение эффективной системы защиты в организации требует настойчивой и целенаправленной повседневной работы. Для создания эффективной системы защиты, прежде всего, необходимо определиться с пониманием слова «система» применительно к организации и осуществлению мероприятий по защите информации.

Любая система состоит из управляющего объекта и объекта управления (рис. 3.1) и создается под заданные требования с учетом существующих ограничений.

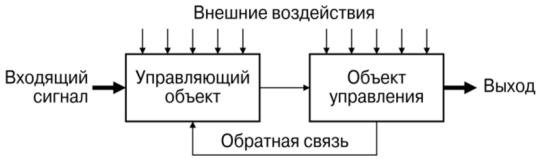


Рис. 3.1. Принципиальная схема системы управления с обратной связью

Всякая система может нормально функционировать только при наличии в ней определенных связей между объектом управления и управляющим объектом. Обязательным для нормального функционирования системы является наличие обратной связи. В общем случае для функционирования любой системы необходимы, прежде всего, побудительные причины, которые могут появиться как от внешнего воздействия, так и от внутренней неудовлетворенности состоянием дел.

Рассмотрим динамику функционирования системы на уровне организации, работающей с категорированной информацией. Так как любая система создается для решения определенного рода задач, то в своем функционировании она ограничивается как объективными, так и субъективными факторами. К ним относятся:

- перечни защищаемых сведений, составляющих государственную и коммерческую тайну;
- требуемые уровни безопасности информации, обеспечение которых не приведет к превышению ущерба над затратами на защиту информации;
- угрозы безопасности информации;
- показатели, по которым будет оцениваться эффективность системы защиты.

Входами системы инженерно-технической защиты информации являются:

- воздействия злоумышленников при физическом проникновении к источникам конфиденциальной информации с целью ее хищения, изменения или уничтожения;
- различные физические поля, электрические сигналы, создаваемые техническими средствами злоумышленников, которые воздействуют на средства обработки и хранения информации;
- стихийные силы, прежде всего пожары, приводящие к уничтожению или изменению информации;
- физические поля и электрические сигналы с информацией, передаваемой по функциональным каналам связи;
- побочные электромагнитные и акустические поля, а также электрические сигналы, возникающие в процессе деятельности объектов защиты и несущие конфиденциальную информацию.

Выходами системы защиты являются меры по защите информации, адекватные входным воздействиям.

Алгоритм процесса преобразования входных воздействий (угроз) в меры защиты и определяет вариант системы защиты.

Порядок функционирования системы защиты информации в организации определяется в руководящих, нормативных и методических документах, выходящих как в вышестоящих организациях, так и разрабатываемых в самой организации.

3.1.2. Руководящие и нормативно-методические документы, регламентирующие деятельность в области защиты информации

К руководящим документам вышестоящих организаций в области защиты информации относятся: «Доктрина информационной безопасности Российской Федерации», утверждена Президентом Российской Федерации 9.09.2000 г. № Пр.-1895; Федеральный закон № 149-ФЗ «Об информации, информационных технологиях и защите информации», от 27 июля 2006 года; Федеральный закон от 16.02.95 г. № 15-ФЗ «О связи»; Федеральный закон от 27.12.2002 г. № 184-ФЗ «О техническом регулировании»; Федеральный закон от 4 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности»; Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных», Указ Президента Российской Федерации от 19.02.99 г. № 212 «Вопросы Государственной технической комиссии при Президенте Российской Федерации»; Указ Президента Российской Федерации от 17.12.97 г. № 1300 «Концепция национальной безопасности Российской Федерации» в редакции указа Президента Российской Федерации от 10.01.2000 г. № 24; Указ Президента Российской Федерации от 06.03.97 г. № 188 «Перечень сведений конфиденциального характера» с дополнениями и изменениями, введёнными Указом Президента Российской Федерации от 23.09.2005 г. № 1111.

К нормативно-методическим документам вышестоящих организаций относятся: Постановление Правительства РФ от 03.02.2012 г. № 79 «Положение о лицензировании деятельности по технической защите конфиденциальной информации»; Постановление от 3 марта 2012 г. № 171 «О лицензировании деятельности по разработке и производству средств защиты конфиденциальной информации»; Постановление Правительства РФ от 16 апреля 2012 г. № 314 «Об утверждении Положения о лицензировании деятельности по выявлению электронных устройств, предназначенных для негласного получения информации (за исключением случая, если указанная деятельность осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)»; Постановление Правительства Российской Федерации от 1.11.2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»; Постановление Правительства Российской Федерации от 03.11.94 г. № 1233 «Положение о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти»; «Сборник руководящих документов по защите информации от несанкционированного доступа» Гостехкомиссия России, Москва,

1998 г.; ГОСТ Р 51275-99 «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения» (новая редакция 2006 г.); ГОСТ Р 50922-96 «Защита информации. Основные термины и определения» (новая редакция 2006 г.); ГОСТ Р 51583-2000 «Порядок создания автоматизированных систем в защищенном исполнении»; ГОСТ Р 51241-98 «Средства и системы контроля и управления доступом. Классификация. Общие технические требования. Методы испытаний»; ГОСТ 12.1.050-86 «Методы измерения шума на рабочих местах»; ГОСТ Р ИСО 7498-1-99 «Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 1. Базовая модель»; ГОСТ Р ИСО 7498-2-99 «Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 2. Архитектура защиты информации»; ГОСТ 2.114-95 «Единая система конструкторской документации. Технические условия»; ГОСТ 2.601-95 «Единая система конструкторской документации. Эксплуатационные документы»; ГОСТ 34.201-89 «Информационная технология. Комплекс стандартов на автоматизированные системы. Виды, комплектность и обозначение документов при создании автоматизированных систем»; ГОСТ 34.602-89 «Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создании автоматизированных систем»; ГОСТ 34.003-90 «Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения»; РД Госстандарта СССР 50-682-89 «Методические указания. Информационная технология. Комплекс стандартов и руководящих документов на автоматизированные системы. Общие положения»; РД Госстандарта СССР 50-34.698-90 «Методические указания. Информационная технология. Комплекс стандартов и руководящих документов на автоматизированные системы. Автоматизированные системы. Требования к содержанию документов»; РД Госстандарта СССР 50-680-89 «Методические указания. Автоматизированные системы. Основные положения»; ГОСТ 34.601-90 «Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадия создания»; ГОСТ 6.38-90 «Система организационно-распорядительной документации. Требования к оформлению»; ГОСТ 6.10-84 «Унифицированные системы документации. Придание юридической силы документам на машинном носителе и машинограмме, создаваемым средствами вычислительной техники, ЕСКД, ЕСПД и ЕСТД»; ГОСТ Р-92 «Система сертификации ГОСТ. Основные положения»; ГОСТ 28195-89 «Оценка качества программных средств. Общие положения»; ГОСТ 28806-90 «Качество программных средств. Термины и определения»; ГОСТ Р ИСОМ-

ЭК 9126-90 «Информационная технология. Оценка программной продукции. Характеристика качества и руководства по их применению»; ГОСТ 2.111-68 «Нормоконтроль»; ГОСТ Р 50739-95 «Средства вычислительной техники. Защита от несанкционированного доступа к информации»; РД Гостехкомиссии России «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля недекларированных возможностей», Москва, 1999 г.; РД Гостехкомиссии России «Средства защиты информации. Специальные общие технические требования, предъявляемые к сетевым помехоподавляющим фильтрам», Москва, 2000 г.; ГОСТ 13661-92 «Совместимость технических средств электромагнитная. Пассивные помехоподавляющие фильтры и элементы. Методы измерения вносимого затухания»; ГОСТ 29216-91 «Совместимость технических средств электромагнитная. Радиопомехи индустриальные от оборудования информационной техники. Нормы и методы испытаний»; ГОСТ 22505-83 «Радиопомехи индустриальные от приемников телевизионных и приемников радиовещательных частотно-модулированных сигналов в диапазоне УКВ. Нормы и методы измерений»; ГОСТ Р 50628-93 «Совместимость электромагнитная машин электронных вычислительных персональных. Устойчивость к электромагнитным помехам. Технические требования и методы испытаний».

Руководствуясь положениями вышеперечисленных документов, ФСТЭК России разработала свои нормативно-методические документы. К ним относятся: ряд методик по оценке защищенности основных технических средств и систем; защищённости информации, обрабатываемой основными техническими средствами и системами, от утечки за счет наводок на вспомогательные технические средства и системы и их коммуникации; защищенности помещений от утечки речевой информации по акустическому и вибрационному каналам; по каналам электроакустических преобразований. Приняты: решение Гостехкомиссии России от 14.03.95 г. № 32 «Типовое положение о Совете (Технической комиссии) министерства, ведомства, органа государственной власти субъекта Российской Федерации по защите информации от иностранных технических разведок и от ее утечки по техническим каналам»; решение Гостехкомиссии России от 03.10.95 г. № 42 «Типовые требования к содержанию и порядку разработки Руководства по защите информации от технических разведок и ее утечки по техническим каналам на объекте» и ряд других документов, которые постоянно, по мере необходимости, разрабатываются специалистами ФСБ и ФСТЭК и внедряются в жизнь. Приказ ФСТЭК России от 11.02.2013 г. № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащей-

ся в государственных информационных системах»; Приказ ФСТЭК России от 18.02.2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

На базе этих документов разрабатываются необходимые руководящие и нормативно-методические документы в организациях.

К руководящим документам, разрабатываемым в организациях, относятся:

- руководство (инструкция) по защите информации в организации;
- положение о подразделении организации, на которое возлагаются задачи по обеспечению безопасности информации;
- инструкции по работе с грифованными документами;
- инструкции по защите информации о конкретных изделиях.

В различных организациях эти документы могут иметь разные наименования, отличающиеся от перечисленных выше. Считаю необходимым напомнить о том, что в пособии речь идет о защите информации, относящейся к информации конфиденциального характера, поэтому жестких требований по характеру и виду документации, разрабатываемых в коммерческих организациях, за исключением отдельных случаев, государственные регуляторы не предъявляют. Но сущность этих документов остается неизменной, так как их наличие в организации объективно.

Порядок защиты информации в организации определяется соответствующим руководством (инструкцией). Руководство должно состоять из следующих разделов:

- общие положения;
- охраняемые сведения об объекте;
- демаскирующие признаки объекта и технические каналы утечки информации;
- оценка возможностей технических разведок и других источников угроз безопасности информации (возможно, спецтехника, используемая преступными группировками);
- организационные и технические мероприятия по защите информации;
- оповещение о ведении разведки (раздел включается в состав Руководства при необходимости);
- обязанности и права должностных лиц;
- планирование работ по защите информации и контролю;
- контроль состояния защиты информации;
- аттестование рабочих мест;
- взаимодействие с другими предприятиями (учреждениями, организациями).

Однако в данном руководстве нельзя учесть всех особенностей защиты информации в конкретных условиях. В любой организации постоянно меняется ситуация с источниками и носителями информации конфиденциального характера, угрозами ее безопасности. Например, появлению нового товара на рынке предшествует большая работа. Она включает различные этапы и стадии: проведение исследований, разработка лабораторных и действующих макетов, создание опытного образца и его доработка по результатам испытаний, подготовка производства (документации, установка дополнительного оборудования, изготовление оснастки — специфических средств производства, необходимых для реализации технологических процессов), изготовление опытной серии для выявления спроса на товар, массовый выпуск продукции.

На каждом этапе и стадии к работе могут подключаться новые люди, разрабатываться новые документы, создаваться узлы и блоки с информативными для них демаскирующими признаками. Созданию каждого изделия или самостоятельного документа сопутствует свой набор информационных элементов, их источников и носителей, угроз и каналов утечки информации, проявляющихся в различные моменты времени.

Для защиты информации об изделии на каждом этапе его создания должна разрабатываться соответствующая инструкция. Инструкция должна содержать необходимые для обеспечения безопасности информации сведения, в том числе:

- общие сведения о наименовании образца;
- защищаемые сведения и демаскирующие признаки;
- потенциальные угрозы безопасности информации;
- замысел и меры по защите;
- порядок контроля (задачи, органы контроля, имеющие право на проверку, средства контроля, допустимые значения контролируемых параметров, условия и методики, периодичность и виды контроля);
- фамилии лиц, ответственных за безопасность информации.

Основным нормативным документом при организации защиты информации является перечень сведений, составляющих государственную, военную, коммерческую или любую другую тайну. Перечень сведений, содержащих государственную тайну, основывается на положениях закона «О государственной тайне». Перечни подлежащих защите сведений, изложенных в этом законе, конкретизируются ведомствами применительно к тематике конкретных организаций.

Перечни сведений, составляющих коммерческую тайну, составляются руководством фирмы при участии сотрудников службы безопасности.

Другие нормативные документы определяют максимально допустимые значения уровней полей с информацией и концентрации демаскирующих веществ на границах контролируемой зоны, которые обеспечивают требуемый уровень безопасности информации. Эти нормы разрабатываются соответствующими ведомствами, а для коммерческих структур, выполняющих негосударственные заказы, — специалистами этих структур.

3.2. Методика принятия решения на защиту от утечки информации в организации

Основная работа по защите информации в организации начинается с принятия руководителем предприятия решения по защите информации. В этом решении определяются основные вопросы организации подготовки и выполнения мероприятий по защите информации. Защита информации проводится всеми сотрудниками предприятия, но степень участия различных категорий существенно отличается и определяется в решении на защиту.

Управленческое решение является результатом знаний, опыта, воли и творчества руководителей, принимающих решения, и в первую очередь главного руководителя (президента, генерального директора), поскольку он утверждает, а зачастую и единолично принимает решение и несет за него всю полноту ответственности. От качества принятого решения зависит построение эффективной защиты от утечки информации, поэтому процессу принятия решения предшествует процесс его выработки. Он включает поиск наилучших путей достижения цели, выявление проблем, требующих немедленного решения.

Таким образом, решение является целеполагающим, исходным моментом, определяющим порядок и характер дальнейшего функционирования управляемого объекта (подчиненных, фирмы и т. д.), постановку ему задач, организацию его взаимодействия с другими системами, всестороннего обеспечения его действий, и тем самым реализация принятого решения обеспечивается организационно.

Если принятие решения — всегда прерогатива начальника, то выработка решения, процесс его поиска и оптимизации — обычно коллективное творчество группы специалистов, заинтересованных в принятии наилучшего решения.

Решение на осуществление деятельности фирмы по тому или иному направлению работы — это результат творческого мышления и форма выражения воли руководства, определяющая цель деятельности, силы и средства, способы и сроки ее достижения, а также ожидаемый конечный результат. Опыт творческой деятельности по выработ-

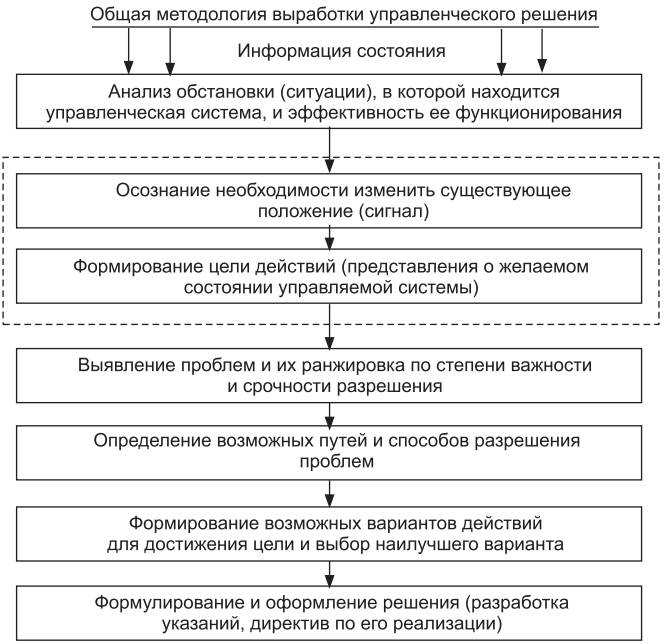


Рис. 3.2. Общая методология выработки управленческого решения

ке решений позволил выработать рациональные способы и приемы его принятия, направленные на облегчение и ускорение этого процесса.

Таким образом, методика выработки решения есть упорядоченная совокупность приемов и способов творческого мышления руководителя, его организаторской деятельности, направленные на своевременную и качественную разработку всех элементов решения.

Наиболее общим подходом к выбору и обоснованию управленческого решения, включающим выбор принципов, форм, средств, логических операций для осуществления процесса выработки решения, является методология выработки управленческого решения (рис. 3.2).

Для каждой конкретной области деятельности на базе общей методологии выработки управленческого решения разработана своя методика принятия решения, учитывающая специфические особенности той сферы деятельности, в которой принимается решение.

3.2.1. Алгоритм принятия решения

Рассмотрим вариант выработки решения на защиту информации. Алгоритм принятия решения на защиту информации представлен на рис. 3.3. Более детально рассмотрим каждый блок, входящий в алгоритм.

Уяснение поставленной задачи является исходным и важным этапом выработки решения. Именно здесь начинает свое рождение основная идея выполнения поставленной задачи, которая на последующих этапах будет углубляться и детализироваться с учетом конкретных особенностей обстановки и возможных ее изменений. Известно, что все явления и процессы окружающего нас мира взаимосвязаны. Эти причинные зависимости порой так обширны и многогранны, что не всегда можно легко и просто их проанализировать, при этом требуется слаженная мыслительная работа. Параллельно с уяснением задачи оценивается обстановка.

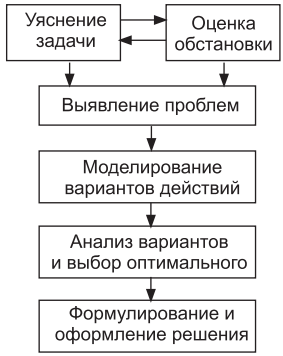


Рис. 3.3. Алгоритм принятия управленческого решения

Оценка обстановки. Под оценкой обстановки в ходе выработки решения понимается установление причинно-следственных связей всех ее элементов и их влияния на выполнение стоящей задачи. Основная цель оценки обстановки состоит в установлении степени влияния различных факторов на успешность выполнения поставленной задачи. При этом руководитель может сделать выводы о том, действия каких факторов следует нейтрализовать как препятствующих выполнению задачи, а действия каких факторов следует использовать как способствующих ее выполнению. В зависимости от содержания поставленной задачи оценка обстановки может проводиться поразному, так как на процесс решения задач могут влиять в той или иной мере абсолютно различные факторы. Наиболее оптимальным представляется следующий вариант оценки обстановки:

- оцениваются потенциальные возможности вероятного противника (злоумышленника);
- свои силы и возможности;
- условия, в которых придется решать поставленные задачи.

Данный вариант оценки дает условное деление на блоки. В реальных условиях оценка производится комплексно, и зачастую бывает невозможно разделить общую оценку обстановки на блоки, так как они тесно взаимосвязаны.

Оценка возможностей вероятного противника (злоумышленника). Львиную долю в организации эффективной защиты от утечки информации по техническим каналам составляет знание возможностей вероятного злоумышленника, интересующегося сведениями, которыми обладает организация. Сложность и особенность оценки вероятного противника заключается в том, что в большинстве случаев не представляется возможным с высокой степенью вероятности точно

определить противостоящую сторону, т. е. мы вынуждены решать слабо определенные или неопределенные проблемы. И здесь на помощь приходит системный подход при решении неопределенных проблем.

Системный подход — это концепция решения сложных слабо определенных или неопределенных проблем, рассматривающая объект изучения (исследования) или проектирования в виде системы.

При применении системного подхода определение возможностей вероятного противника (злоумышленника) будет являться одним из элементов системы, оценка которых сводится к моделированию действий вероятного противника. В дальнейшем результаты моделирования ложатся в основу разработки системы защиты организации.

Моделирование действий вероятного противника, направленных на добывание информации, предусматривает анализ способов ее хищения, изменения и уничтожения с целью оценки наносимого этими способами ущерба. Оно включает моделирование способов физического проникновения злоумышленника к источникам информации и моделирование технических каналов утечки информации.

Действия злоумышленника по добыванию информации, так же как и других материальных ценностей, определяются поставленными целями и задачами, его мотивами, квалификацией и технической оснащенностью. Так же как в криминалистике, расследование преступления начинается с ответа на вопрос: кому это выгодно, так и прогноз способов физического проникновения следует начать с выяснения: кому нужна защищаемая информация. Способы проникновения исполнителей зарубежных спецслужб будут отличаться высокими квалификацией и технической оснащенностью; конкурентов — подготовленными исполнителями со средствами, имеющимися на рынке; криминальных структур — достаточно подготовленными и хорошо оснащенными исполнителями.

Для создания модели угрозы физического проникновения, достаточно близкой к реальной, необходимо «перевоплотиться» в злоумышленника, т. е. попытаться мысленно проиграть с позиции злоумышленника варианты проникновения к источнику информации. Чем больше при этом будет учтено факторов, влияющих на эффективность проникновения, тем выше адекватность модели. В условиях отсутствия информации о злоумышленнике, его квалификации, технической оснащенности во избежание грубых ошибок лучше переоценить угрозу, чем ее недооценить, хотя такой подход может привести к увеличению затрат на защиту.

На основе такого подхода модель злоумышленника выглядит следующим образом:

- злоумышленник представляет серьезного противника, тщательно готовящего операцию проникновения, он изучает обстановку вок-

руг территории организации, наблюдаемые механические преграды, средства охраны, телевизионного наблюдения и дежурного (ночного) освещения, а также сотрудников с целью добывания от них информации о способах и средствах защиты;

- имеет в распоряжении современные технические средства проникновения и преодоления механических преград;
- всеми доступными способами добывает и анализирует информацию: о расположении зданий и помещений организации, о рубежах охраны, о местах хранения источников информации, видах и типах средств охраны, телевизионного наблюдения, освещения и местах их установки;
- проводит анализ возможных путей проникновения к источникам информации и ухода после выполнения задачи.

В зависимости от квалификации, способов подготовки и физического проникновения в организацию злоумышленников разделяют на следующие типы:

- неподготовленный, который ограничивается внешним осмотром объекта, проникает в организацию через двери и окна, при срабатывании тревожной сигнализации убегает;
- подготовленный, изучающий систему охраны объекта и готовящий несколько вариантов проникновения в организацию, в основном с помощью взлома инженерных конструкций;
- квалифицированный, который тщательно готовится к проникновению, выводит из строя технические средства охраны, применяет наиболее эффективные способы проникновения.

При моделировании действий квалифицированного злоумышленника необходимо также исходить из предположения, что он хорошо представляет современное состояние технических средств защиты информации, типовые варианты их применения, слабые места и «мертвые» зоны диаграмм направленности активных средств охраны [98].

Возможные пути проникновения злоумышленников отмечаются линиями на платах (схемах) территории, этажей и помещений зданий, а результаты анализа пути заносятся в табл. 3.1.

Следующим элементом системы является **оценка своей организации** как возможного источника информации для противника. При этом оценка начинается с анализа возможных каналов утечки информации.

Все ТКУИ можно разделить по физической природе появления на естественные и искусственно созданные.

Естественные каналы обусловлены физическими полями, которые сопровождают нормальные процессы и воздействуют на окружающие объекты. В данном случае речь идет о явлениях помех, существующих помимо воли и желаний как владельца информации, так и

Таблица 3.1

№ элемента информации	Цена информации	Путь проникновения злоумышленника	Оценка реальности пути	Величина угрозы	Ранг угрозы
1	2	3	4	5	6

потенциального злоумышленника. Пример таких каналов — возникновение микрофонных эффектов, акустические и вибрационные каналы.

Искусственно созданные каналы являются рукотворными. Для их организации в помещение или в технические средства могут внедряться те или иные электронные компоненты устройств съема или дорабатываться сами объекты с целью усиления требуемых свойств.

Задачи выявления естественных и искусственных каналов отличаются.

При выявлении первых стоит задача выявить саму физическую возможность съема информации, т. е. обнаружить физическое поле, содержащее информативную составляющую, оценить соотношение полезный сигнал/шум в раздведдоступной точке (или точках, если таких несколько).

При выявлении вторых речь идет об обнаружении непосредственно физического тела (схемы, компонента) устройства съема или демаскирующих признаков работ по усилению естественных свойств информационных полей.

Таким образом, как правило, естественные каналы выявляются в процессе измерений параметров полей, а искусственные в процессе сложного комбинированного процесса анализа полей и физического поиска.

При этом возникает необходимость определения всей совокупности каналов утечки информации.

Если, A — каналы утечки акустической речевой информации; $O_{\text{об}}$ — каналы утечки обрабатываемой ТС информации; C — каналы утечки информации, передаваемой по каналам связи; B — каналы утечки видовой (графической, текстовой и др.) информации, а K — совокупность всех каналов утечки информации ($K_{\text{у}}$), тогда

$$K_{\text{у}} = A + O_{\text{об}} + C + B = \sum\{A, O_{\text{об}}, C, B\}.$$

Обозначив для квантора общности объекта информатизации $\text{М}\exists K_{\text{м}}$ — каналы утечки информации на объекте, получим, что $[K_{\text{м}}] \to \infty$, т. е. потенциально возможные каналы утечки информации постоянно будут расти в зависимости от развития техники и наших научных знаний в этой области. Выявление всех каналов утечки информации практически невозможно и экономически нецелесообразно.

При оценке своей организации с целью решения вопросов информационной безопасности (ИБ) основной задачей является выделение из $K_{\text{м}}$ некоего $K'_{\text{м}}$ — множества наиболее потенциально опасных каналов утечки ($K_{\text{у}}$). Выбор $K'_{\text{м}}$ зависит от ряда факторов и может изменяться в зависимости от стоящих задач.

Основной целью при определении наиболее потенциально опасных $K_{\text{у}}$ является уход от бессмысленных работ по выявлению всех кванторов (логических операций) существования всех $K_{\text{у}}$. То есть наша задача выделить факторы для защищаемого объекта на период защиты, которые определяют функционирование наиболее потенциально опасных $K_{\text{у}}$.

Факторы, определяющие $K'_{\text{м}}$, определяются непосредственно владельцем информации или службой, на которой возложена такая задача. Даже при привлечении сторонних организаций окончательное решение — за собственником (владельцем) информации.

Фактически, определяя каналы утечки, мы определяем весь спектр возможных действий технической разведки противника по отношению к защищаемым информационным ресурсам объекта, т. е. моделируем возможности противника.

Обнаружение и распознавание каналов утечки информации, так же как и любых объектов, производится по их демаскирующим признакам. В качестве достаточно общих признаков, дающих потенциальную возможность несанкционированного получения информации в зависимости от вида каналов утечки информации, могут служить приведенные ниже признаки.

Для оптического канала: окна, выходящие на улицу, близость к ним противоположных домов и деревьев. Отсутствие на окнах занавесок, штор, жалюзи. Просматриваемость содержания документов на столах со стороны окон, дверей, шкафов в помещении. Просматриваемость содержания плакатов на стенах помещения для совещания из окон и дверей. Малое расстояние между столами сотрудников в помещении. Просматриваемость экранов мониторов ПЭВМ на столах сотрудников со стороны окон, дверей или других сотрудников. Складирование продукции во дворе без навесов. Малая высота забора и дырки в нем. Переноска и перевозка образцов продукции в открытом виде. Появление возле территории организации (предприятия) посторонних людей (в том числе в автомобилях) с биноклями, фотоаппаратами, кино- и видеокамерами. Выход окон помещения на улицу, близость к ним улицы и противоположных домов.

Для канала ПЭМИН и электрических каналов: наличие в помещении радиоэлектронных средств, ПЭВМ, ТА городской и внутренней АТС, громкоговорителей трансляционной сети и других технических средств. Применение средств радиосвязи. Параллельное размещение

кабелей в одном жгуте при разводке их внутри здания и на территории организации. Доступность или неоптимальное построение и размещение систем электропитания и заземления ТС. Параллельное размещение кабелей в одном жгуте при разводке их внутри здания и на территории организации. Длительная и частая парковка возле организации чужих автомобилей, в особенности с сидящими в машине людьми.

Для акустического и вибрационного каналов: малая толщина дверей и стен помещения. Выход ограничивающих конструкций помещений (стены, перекрытия пола и/или потолка) в сторонние помещения. Наличие в помещении открытых вентиляционных отверстий и общая со сторонними помещениями система вентиляции. Выход труб систем отопления и водоснабжения за пределы контролируемой зоны. Близость окон к улице и ее домам. Появление возле организации людей с достаточно большими сумками, длинными и толстыми зонтами. Частая и продолжительная парковка возле организации чужих автомобилей.

Для материально-вещественного канала: отсутствие закрытых и опечатанных ящиков для бумаги и твердых отходов с демаскирующими веществами. Применение радиоактивных веществ. Неконтролируемый выброс газов с демаскирующими веществами, слив в водоемы и вывоз на свалку твердых отходов. Запись сотрудниками конфиденциальной информации на неучтенных листах бумаги.

Приведенные признаки являются лишь ориентирами при поиске потенциальных каналов утечки. В конкретных условиях их состав существенно больший.

Потенциальные каналы утечки определяются для каждого источника информации, причем их количество может не ограничиваться одним или двумя. Например, от источника информации — руководителя фирмы — утечка информации возможна по следующим каналам:

- через дверь в приемную или коридор;
- через окно на улицу или во двор;
- через вентиляционное отверстие в соседние помещения;
- с опасными сигналами по радиоканалу;
- с опасными сигналами по кабелям, выходящим из помещения;
- по трубам отопления в другие помещения здания;
- через стены, потолок и пол в соседние помещения;
- с помощью закладочных устройств за территорию фирмы.

Моделирование технических каналов утечки информации по существу является единственным методом достаточно полного исследования их возможностей с целью последующей разработки способов и средств защиты информации. В основном применяются вербальные и математические модели.

Физическое моделирование каналов утечки затруднено и часто невозможно по следующим причинам:

- приемник сигнала канала является средством злоумышленника, его точное месторасположение и характеристики службе безопасности неизвестны;
- канал утечки включает разнообразные инженерные конструкции (бетонные ограждения, здания, заборы и др.) и условия распространения носителя (переотражения, помехи и т. д.), воссоздать которые на макетах невозможно или для этого потребуются огромные расходы.

Применительно к моделям каналов утечки информации целесообразно иметь модели, описывающие каналы в статике и динамике.

Статическое состояние канала характеризуют структурная и пространственная модели. Структурная модель описывает структуру (состав и связи элементов) канала утечки. Пространственная модель содержит описание положения канала утечки в пространстве:

- места расположения источника и приемника сигналов, удаленность их от границ территории организации;
- как ориентирован вектор распространения носителя информации в канале утечки информации и его протяженность.

Структурную модель канала целесообразно представлять в табличной форме, пространственную — в виде графа на плане помещения, здания, территории организации, прилегающих внешних участков среды. Структурная и пространственная модели не являются автономными, а взаимно дополняют друг друга.

Динамику канала утечки информации описывают функциональная и информационная модели. Функциональная модель характеризует режимы функционирования канала, интервалы времени, в течение которых возможна утечка информации, а информационная содержит характеристики информации, утечка которой возможна по рассматриваемому каналу: количество и ценность информации, пропускная способность канала, прогнозируемое качество принимаемой злоумышленником информации.

Указанные модели объединяются и увязываются между собой в рамках комплексной модели канала утечки. В ней указываются интегральные параметры канала утечки информации: источник информации и её вид, источник сигнала, среда распространения и её протяженность, ориентировочное место размещения приемника сигнала, информативность канала и величина угрозы безопасности информации.

Каждый вид канала содержит свой набор показателей источника и приемника сигналов в канале, позволяющих оценить максимальную

дальность канала и показатели возможностей органов государственной и коммерческой разведки.

Так как приемник сигнала является принадлежностью злоумышленника и точное место его размещения и характеристики не известны, то моделирование канала проводится применительно к гипотетическому приемнику. В качестве приемника целесообразно рассматривать приемник, параметры которого соответствуют современному уровню, а место размещения выбрано рационально. Уважительное отношение к интеллекту и техническим возможностям противника гарантирует от крупных ошибок в значительно большей степени, чем пренебрежительное.

При описании приемника сигнала необходимо учитывать реальные возможности злоумышленника. Очевидно, что приемники сигналов коммерческой разведки не могут, например, размещаться на космических аппаратах.

Что касается технических характеристик средств добывания информации, то они для государственной и коммерческой разведки существенно не отличаются. Расположение приемника злоумышленника можно приблизительно определить исходя из условий обеспечения значения отношения сигнал/помеха на входе приемника, необходимого для съема информации с допустимым качеством, и безопасности злоумышленника или его аппаратуры.

Если возможное место размещения приемника сигналов выбрано, то в ходе моделирования канала рассчитывается энергетика носителя на входе приемника с учетом мощности носителя на выходе источника, затухания его в среде распространения, уровня помех, характеристик сигнала и его приемника. Например, разрешение при фотографировании находящихся в служебном помещении людей и предметов из окна противоположного дома легко оценить по известной формуле

$$H = hL/f,$$

где h — разрешение в долях миллиметра системы «объектив— фотопленка»; f — фокусное расстояние телеобъектива фотоаппарата; L — расстояние от объекта наблюдения до фотоаппарата. Если фотографирование производится фотоаппаратом «Фотоснайпер ФС-122» с $f = 300$ мм и $h = 0{,}03$ мм (разрешение 33 лин/мм), то для $L = 50$ м, H равно 5 мм. Учитывая, что для обнаружения и распознавания объекта его изображение должно состоять из не менее 9 точек, то минимальные размеры объекта 15×15 мм. Очевидно, что на фотографии можно будет рассмотреть человека, продукцию, но нельзя прочитать машинописный текст на бумаге или экране монитора.

Все выявленные потенциальные каналы утечки информации и их характеристики записываются в табл. 3.2. В графе 4 указываются

Таблица 3.2

№ элемента информации	Цена информации	Источник сигнала	Путь утечки информации	Вид канала	Оценки реальности канала	Величина угрозы	Ранг угрозы
1	2	3	4	5	6	7	8

основные элементы среды распространения и возможные места размещения приемника сигналов. По физической природе носителя определяется вид канала утечки информации.

Оценка показателей угроз безопасности представляет достаточно сложную задачу в силу следующих обстоятельств:

- добывание информации нелегальными путями не афишируется и фактически отсутствуют или реальные статистические данные по видам угроз безопасности информации очень скудно представлены в литературе. Кроме того, следует иметь ввиду, что характер и частота реализации угроз зависят от криминогенной обстановки в районе нахождения организации, и данные об угрозах, например, в странах с развитой рыночной экономикой, не могут быть однозначно использованы для российских условий;
- оценка угроз безопасности информации основывается на прогнозе действий органов разведки. Учитывая скрытность подготовки и проведения разведывательной операции, их прогноз приходится проводить в условиях острой информационной недостаточности;
- многообразие способов, вариантов и условий доступа к защищаемой информации существенно затрудняют возможность выявления и оценки угроз безопасности информации. Каналы утечки информации могут распространяться на достаточно большие расстояния и включать в качестве элементов среды распространения труднодоступные места;
- априори не известен состав, места размещения и характеристики технических средств добывания информации злоумышленника.

Оценки угроз информации в результате проникновения злоумышленника к источнику или ее утечки по техническому каналу носят вероятностный характер. При этом рассматривается вероятность $P_{\text{р}}$ реализуемости рассматриваемого пути или канала, а также цены соответствующего элемента информации $C_{\text{и}}$.

Угроза безопасности информации, выраженной в величине ущерба $C_{\text{уи}}$ от попадания ее к злоумышленнику, определяется для каждого пути или канала в виде

$$C_{\text{уи}} = C_{\text{и}} P_{\text{р}}.$$

Моделирование угроз безопасности информации завершается их ранжированием.

На каждый потенциальный способ проникновения злоумышленника к источнику информации и канал утечки информации целесообразно завести карточки, в которые заносятся в табличной форме характеристики моделей канала. Структурная, пространственная, функциональная и информационная модели являются приложениями к комплексной модели канала утечки. На этапе разработки способов и средств предотвращения проникновения злоумышленника и утечки информации по рассматриваемому каналу к карточкам добавляется приложение с перечнем мер по защите и оценками затрат на нее [96].

Более удобным вариантом является представление моделей на основе машинных баз данных, математическое обеспечение которых позволяет учесть связи между разными моделями, быстро корректировать данные в них и систематизировать каналы по различным признакам, например по виду, положению в пространстве, способам и средствам защиты, угрозам.

Оценка условий, в которых придется решать поставленную задачу. Оценка условий, в которых придется решать поставленную задачу, происходит в комплексе совместно с оценкой вероятного противника и своей организации, так как невозможно качественно смоделировать процесс, отрывая его от условий, в которых он происходит. Выделение оценки условий в отдельный параграф позволяет избежать возможных упущений при комплексной оценке обстановки.

При оценке условий прежде всего:

- анализируется расположение объекта на местности с учетом окружающей его территории и размещенных на ней посторонних объектов;
- оценивается контролируемая зона и возможности по снятию информации из-за ее пределов;
- обследуется сам защищаемый объект.

При непосредственном знакомстве с защищаемым объектом прежде всего выясняют:

- взаимное расположение контролируемых и смежных помещений, режимы их посещения;
- устанавливают факты и сроки ремонтных работ, монтажа и демонтажа коммуникаций, замены предметов мебели и интерьера;
- изготовляют планы помещений, на которые наносят все входящие и проходящие коммуникации;
- изучают конструктивные особенности ограждающих поверхностей, материалы покрытий.

Особое внимание в условиях плотной застройки уделяют подготовке плана прилегающей территории, которая может быть исполь-

зована для парковки автомобилей с приемной радиоаппаратурой, развертывания систем видеонаблюдения или дистанционного аудиоконтроля.

Результаты проведенного анализа в конечном счете составляют основу **модели вероятного противника,** исходя из которой строится концепция защиты любого объекта.

Модель позволяет учитывать:

- типы и состав защищаемых информационных ресурсов (ИР) объекта;
- значимость (стоимость) каждого из ИР;
- оперативные возможности противника;
- технические возможности противника;
- финансовые возможности противника;
- порядок эксплуатации объекта и уже реализованные меры обеспечения безопасности информации (организационные, режимные, инженерные, технические), затрудняющие или делающие невозможным съем информации по тому или иному каналу.

На основании перечисленных исходных данных модель описывает весь объем каналов утечки, считающихся потенциально опасными.

Таким образом, **модель вероятного противника** является основным руководящим документом для организации жизнедеятельности самого объекта, а также определяет и регламентирует действия технических служб по обеспечению его безопасности.

Результат оценки обстановки в виде полученной модели вероятного противника позволяет выявить и произвести ранжировку проблем, стоящих перед руководителем при решении вопроса об организации и осуществления защиты от утечки информации по техническим каналам.

Ранее уже упоминалось, что в теории решений под проблемой понимается всякое различие между имеющимся и необходимым положением дел. Всякая попытка устранить это различие, естественно, связана с определенными трудностями. Различный уровень этих трудностей и обусловил наличие нескольких типов проблем: *стандартных, хорошо определенных, слабо определенных, неопределенных.*

Однако в практике управления руководитель, как правило, не задумывается о том, с каким типом проблем он имеет дело. В проблеме он прежде всего видит трудности на пути достижения поставленной цели, разрешение которых не лежит на поверхности, а требует от руководителя принятия особых мер, выходящих за пределы привычных стандартных действий. А так как разрешение всякой проблемы связано с необходимостью затраты определенных сил и средств, то очень важно выявить в первую очередь истинные, а не ложные проблемы, чтобы своевременно их разрешить.

Разрешить проблему — значит найти те действия, с помощью которых состояние системы (объекта) управления изменится с действительного на желаемое, которое и является целью действий. Каждая выявленная проблема должна быть четко сформулирована. Закончив выявление проблем, руководитель должен осуществить их ранжировку, т. е. каждой выявленной проблеме определить место (ранг) в ряду других по важности, а значит и степень срочности ее разрешения. При этом могут возникнуть следующие вопросы:

- какую из проблем следует считать главной?
- как разрешить противоречия между ними?
- чем поступиться, если противоречие неразрешимо?

Для определения важности выявленных проблем и места каждой из них можно воспользоваться ответом на следующий вопрос: *«Что будет, если проблема не будет решена?»* Ответ на этот вопрос позволит в полной мере оценить важность и актуальность решения той или иной проблемы. Теперь, когда руководителю стало ясно, какие проблемы и в какой последовательности необходимо решить, он уже может выбрать конкретный метод своей работы и определить, какой круг вопросов должен решить сам, а какие вопросы можно поручить специалистам отдела (службы, фирмы). При этом определяются сроки подачи предложений по разрешению поставленных им задач.

3.2.2. Разработка вариантов и выбор оптимального

На заключительной стадии оценки обстановки все найденные пути решения проблем обобщаются и синтезируются руководителем в возможные варианты решения стоящей задачи для достижения цели действий и затем из них выбирается наилучший, позволяющий достичь поставленной цели действий с наименьшими затратами сил и средств и более качественно. Из анализа практических решений по защите информации можно сделать вывод, что возможных вариантов решения поставленной задачи, обеспечивающих ее успешное выполнение, не так уж много — максимум 4–6. При наличии нескольких таких возможных вариантов задача руководителя выбрать такой, который при безусловном достижении поставленной цели обеспечит максимальную эффективность работ. Для этого необходимо оценить выбранные варианты и определить среди них наиболее подходящий для конкретных условий вариант. На практике применяются два подхода к выбору оптимального варианта:

- сравниваются несколько вариантов;
- анализируется один вариант, но он выбирается по этапам (шагам).

Однако при использовании того или другого подхода возникает необходимость сравнения вариантов или различных элементов (шагов) одного варианта для выбора из них лучшего. Для этой цели

приходится использовать какие-то критерии (в переводе с греческого «мерило») для качественной оценки рассматриваемых вариантов. В качестве критериев выбираются такие показатели, которые наиболее полно характеризуют оцениваемый процесс.

При этом может использоваться несколько способов выбора оптимального варианта действий:

1 вариант: выбирается критерий, наиболее полно отражающий степень достижения цели действий, и по нему сравнивают предлагаемые варианты.

2 вариант: задаются определенные ограничения значений критериев. Затем варианты, не удовлетворяющие критериям с введенными ограничениями, отбрасываются, а из оставшихся вариантов выбирается наилучший по максимуму значений используемых критериев.

3 вариант: задается удельный вес (коэффициент значимости) каждому критерию и выбирается обобщенный критерий эффективности.

4 вариант: ранжировка вариантов по выбранным критериям эффективности.

Решение проблемы защиты информации с точки зрения системного подхода можно сформулировать как трансформацию существующей системы в требуемую.

Целями системы защиты являются обеспечение требуемых уровней безопасности информации на фирме, в организации, на предприятии (в общем случае — на объекте защиты). Задачи конкретизируют цели применительно к видам и категориям защищаемой информации, а также элементам объекта защиты и отвечают на вопрос, что надо сделать для достижения целей. Кроме того, уровень защиты нельзя рассматривать в качестве абсолютной меры, безотносительно от ущерба, который может возникнуть от потери информации и использования ее злоумышленником во вред владельцу информации.

В качестве критериев при выборе рационального варианта для оценки требуемого уровня защиты целесообразно выбрать соотношение между ценой защищаемой информации и затратами на ее защиту. Уровень защиты рационален, когда обеспечивается требуемая степень безопасности информации и минимизируются расходы на ее защиту. Эти расходы $C_{\text{ри}}$ складываются из:

- затрат на защиту информации $C_{\text{зи}}$;
- ущерба $C_{\text{уи}}$ за счет попадания информации к злоумышленнику и использования ее во вред владельцу.

Между этими слагаемыми существует достаточно сложная связь, так как ущерб из-за недостаточной безопасности информации уменьшается с увеличением расходов на ее защиту. Если первое слагаемое может быть точно определено, то оценка ущерба в услови-

ях скрытности разведки и неопределенности прогноза использования злоумышленником полученной информации представляет достаточно сложную задачу. Ориентировочная оценка ущерба возможна при следующих допущениях.

Владелец информации ожидает получить от ее материализации определенную прибыль, которой он может лишиться в случае попадания ее конкуренту. Кроме того, последний, используя информацию, может нанести владельцу еще дополнительный ущерб за счет, например, изменения тактики продажи или покупки ценных бумаг и т. д. Дополнительные неблагоприятные факторы чрезвычайно трудно поддаются учету. Поэтому в качестве граничной меры для оценки ущерба можно использовать потенциальную прибыль $C_{\text{пп}}$, которую ожидает получить от информации ее владелец, т. е.

$$C_{\text{уи}} \geqslant C_{\text{пп}}.$$

В свою очередь ущерб зависит от уровня защиты, который определяется расходами на нее. Максимальный ущерб возможен при нулевых расходах на защиту, гипотетический нулевой обеспечивается при идеальной защите. Но идеальная защита требует бесконечно больших затрат.

При увеличении расходов на защиту вероятность попадания информации злоумышленнику, а следовательно, и ущерб уменьшаются. При этом рост суммарных расходов на информацию с увеличением затрат на ее защиту имеет место в период создания или модернизации системы, когда происходит накопление мер и средств защиты, которые еще не оказывают существенного влияния на безопасность информации. Например, предотвращение утечки информации по отдельным каналам без снижения вероятности утечки по всем остальным не приводит к заметному повышению безопасности информации, хотя затраты на закрытие отдельных каналов могут быть весьма существенными. Образно говоря, для объекта защиты существует определенная «критическая масса» затрат на защиту информации, при превышении которой эти затраты обеспечивают эффективную отдачу.

При некоторых рациональных затратах на защиту информации выше критических наблюдается оптимум суммарных расходов на защиту. При затратах ниже рациональных увеличивается потенциальный ущерб за счет повышения вероятности попадания конфиденциальной информации к злоумышленнику, при более высоких затратах — увеличиваются прямые расходы на защиту.

Ограничения системы представляют собой выделяемые на защиту информации людские, материальные, финансовые ресурсы, а также ограничения в виде требований к системе. Суммарные ресурсы

удобно выражать в денежном эквиваленте. Независимо от выделяемых на защиту информации ресурсов, они не должны превышать суммарной цены защищаемой информации. Это верхний порог ресурсов.

Ограничения в виде требований к системе предусматривают принятие таких мер по защите информации, которые не снижают эффективность функционирования системы при их выполнении. Например, можно настолько ужесточить организационные меры управления доступом к источникам информации, что наряду со снижением возможности ее хищения или утечки ухудшатся условия выполнения сотрудниками своих функциональных обязанностей.

При оценке вариантов защиты информации наиболее целесообразно использовать 3-й вариант, когда задается удельный вес (коэффициент значимости) каждому критерию и выбирается обобщенный критерий эффективности.

В качестве этого критерия может быть использован обобщенный критерий в виде отношения эффективность/стоимость, учитывающий основные характеристики системы, или представлять собой набор частных показателей.

В качестве частных показателей критерия эффективности системы защиты информации используются, в основном, те же, что и при оценке эффективности разведки. Это возможно потому, что цели и задачи, а следовательно, значения показателей эффективности разведки и защиты информации близки по содержанию, но противоположны по результатам. То, что хорошо для безопасности информации, плохо для разведки, и наоборот.

Частными показателями эффективности системы защиты информации являются:

- вероятность обнаружения и распознавания органами разведки объектов защиты;
- погрешности измерения признаков объектов защиты;
- качество (разборчивость) речи на выходе приемника злоумышленника;
- достоверность (вероятность ошибки) дискретного элемента информации (буквы, цифры, элемента изображения).

Очевидно, что система защиты тем эффективнее, чем меньше вероятность обнаружения и распознавания объекта защиты органом разведки (злоумышленником), чем ниже точность измерения им признаков объектов защиты, ниже разборчивость речи, выше вероятность ошибки приема органом разведки дискретных сообщений.

Однако при сравнении вариантов построения системы по нескольким частным показателям возникают проблемы, обусловленные возможным противоположным характером изменения значений разных

показателей: одни показатели эффективности одного варианта могут превышать значения аналогичных показателей второго варианта, другие наоборот — имеют меньшие значения. Какой вариант предпочтительнее? Кроме того, важным показателем системы защиты являются затраты на обеспечение требуемых значений оперативных показателей. Поэтому результаты оценки эффективности защиты по совокупности частных показателей, как правило, неоднозначные.

Для выбора рационального (обеспечивающего достижение целей, решающего поставленные задачи при полном наборе входных воздействий с учетом ограничений) варианта с помощью сравнения показателей нескольких вариантов используется обобщенный критерий в виде отношения эффективность/стоимость. Под эффективностью понимается степень выполнения системой задач, под стоимостью — затраты на защиту.

В качестве критерия эффективности $K_э$ применяются различные композиции частных показателей, чаще их «взвешенная» сумма:

$$K_э = \sum \alpha_i K_i,$$

где α_i — «вес» частного показателя эффективности K_j.

Вес частного показателя определяется экспертами (руководством, специалистами организации, сотрудниками службы безопасности) в зависимости от характера защищаемой информации. Если защищается в основном семантическая информация, то больший вес имеют показатели оценки разборчивости речи и вероятности ошибки приема дискретных сообщений. В случае защиты объектов наблюдения выше вес показателей, характеризующих вероятности обнаружения и распознавания этих объектов.

Для оценки эффективности системы защиты информации по указанной формуле частные показатели должны иметь одинаковую направленность влияния на эффективность — при увеличении их значений повышается значение эффективности. С учетом этого требования в качестве меры обнаружения и распознавания объекта надо использовать вероятность необнаружения и нераспознания, а вместо меры качества подслушиваемой речи — ее неразборчивость. Остальные частные показатели соответствуют приведенным выше.

Выбор лучшего варианта производится по максимуму обобщенного критерия, так как он имеет в этом случае лучшее соотношение эффективности и стоимости. Затем выбранные варианты, которые соответствуют наиболее рациональному построению и организации защиты, предлагаются руководству.

После рассмотрения руководством предлагаемых вариантов (лучше двух для предоставления выбора), учета предложений и замеча-

ний, наилучший, с точки зрения лица принимающего решения, вариант ложится в основу замысла решения руководителя на организацию защиты информации на фирме (объектах защиты). В нем руководитель намечает порядок и последовательность решения проблем, влияющих на выполнение основной задачи, при этом он определяет:

- ответственных за выполнение основных этапов работ;
- последовательность и сроки их выполнения;
- порядок финансирования и материального обеспечения;
- порядок и последовательность действий при отклонениях и несоблюдении сроков решения основных вопросов;
- порядок взаимодействия отделов и служб фирмы;
- порядок управления и контроля за действиями подчиненных.

После оформления решения отрабатывается план-график выполнения работ, в котором отражаются основные вопросы решения:

- начало и окончание основных работ;
- ответственные исполнители;
- последовательность выполнения и взаимосвязь основных этапов;
- организация контроля качества и сроков выполнения основных видов работ.

В процессе реализации решения в результате изменения обстановки возможно внесение корректив в план-график выполнения работ и уточнение основных этапов, которые не должны влиять на сроки достижения конечной цели, а следовательно, при принятии решения эти факторы должны учитываться при определении сроков достижения окончательной цели действий.

3.3. Организация защиты информации

В организациях работа по инженерно-технической защите информации, как правило, состоит из двух этапов:

- построение или модернизация системы защиты;
- поддержание защиты информации на требуемом уровне.

Построение системы защиты информации проводится во вновь создаваемых организациях, в остальных — модернизация существующей.

В зависимости от целей, порядка проведения и применяемого оборудования методы и способы защиты информации от утечки по техническим каналам можно разделить на организационные, поисковые и технические.

Организационные способы защиты. Эти меры осуществляются без применения специальной техники и предполагают следующее:

- установление контролируемой зоны вокруг объекта;

- введение частотных, энергетических, временны́х и пространственных ограничений в режимы работы технических средств приема, обработки, хранения и передачи информации (ТСПИ, ОТСС);
- отключение на период проведения закрытых совещаний вспомогательных технических средств и систем (ВТСС), обладающих качествами акустоэлектрических преобразователей (телефон, факс и т. п.), от соединительных линий;
- применение только сертифицированных ТСПИ, ОТСС и ВТСС;
- привлечение к строительству и реконструкции выделенных (защищенных) помещений, монтажу аппаратуры ТСПИ и ОТСС, а также к работам по защите информации исключительно организаций, лицензированных соответствующими службами на деятельность в данной области;
- категорирование и аттестование объектов информатизации и выделенных помещений на соответствие требованиям обеспечения защиты информации при проведении работ со сведениями различной степени секретности;
- режимное ограничение доступа на объекты размещения ТСПИ, ОТСС и в выделенные помещения.

Необходимо отметить, что все перечисленные меры направлены на решение всё той же единой задачи — добиться получения необходимого отношения сигнал/шум на границе КЗ. Этой задаче подчинены все перечисленные меры, начиная с установления границ КЗ (так, чтобы на них это требование выполнялось) до отключения оборудования (т. е. обеспечения нулевой мощности опасного сигнала).

Поисковые мероприятия. Портативные подслушивающие (закладочные) устройства выявляют в ходе специальных обследований и проверок. Обследование объектов размещения ТСПИ и выделенных помещений выполняется без применения техники с помощью визуального осмотра. В ходе спецпроверки, выполняемой с применением пассивных (приемных) и активных поисковых средств, осуществляется:

- контроль радиоспектра и побочных электромагнитных излучений ТСПИ;
- выявление с помощью аппаратно-программных комплексов, сканеров, индикаторов электромагнитного поля и другой поисковой аппаратуры, негласно установленных подслушивающих приборов;
- специальная проверка выделенных помещений, ТСПИ и ВТСС с использованием нелинейных локаторов и мобильных рентгеновских установок.

Техническая защита. Подобные мероприятия проводятся с применением как пассивных, так и активных защитных приемов и средств.

К пассивным техническим способам защиты относят:

- установку систем ограничения и контроля доступа на объектах размещения ТСПИ, ОТСС и в выделенных помещениях;
- экранирование ТСПИ, ОТСС и их соединительных линий;
- правильное заземление ТСПИ, ОТСС и экранов соединительных линий приборов;
- звукоизоляцию выделенных помещений;
- встраивание в ВТСС, обладающих «микрофонным» эффектом и имеющих выход за пределы контролируемой зоны, специальных устройств защиты;
- ввод автономных и стабилизированных источников, а также устройств гарантированного питания в цепи электроснабжения ТСПИ и ОТСС;
- монтаж в цепях электропитания ТСПИ, ОТСС, а также в электросетях выделенных помещений помехоподавляющих фильтров.

Активное воздействие на каналы утечки осуществляют реализацией:

- пространственного и линейного зашумления, создаваемого генераторами электромагнитного и электрического шума;
- прицельных помех, генерируемых на рабочих частотах радиоканалов подслушивающих устройств специальными передатчиками;
- акустических и вибрационных помех, генерируемых системами вибрационной и акустической защиты;
- подавления диктофонов устройствами направленного высокочастотного радиоизлучения.

Контрольные вопросы для самостоятельной работы

1. Основные требования, предъявляемые к защите информации.
2. Определите принципиальную схему системы управления объектом и взаимосвязь ее элементов.
3. Перечислите руководящие документы в области защиты информации.
4. Структура «Доктрины информационной безопасности РФ».
5. Структура руководства по защите информации в организации.
6. Алгоритм принятия решения на защиту информации.
7. Особенности оценки обстановки при принятии решения на организацию защиты информации.
8. Основные вопросы, рассматриваемые при оценке вероятного противника.
9. Особенности выполнения работ по выявлению искусственных и естественных каналов утечки информации.
10. Основные демаскирующие признаки радиоэлектронного канала утечки.
11. Основные демаскирующие признаки аккустического канала утечки информации.
12. Особенности оценки условий, в которых придется решать задачу по защите информации.
13. Какие вопросы позволяет учитывать модель вероятного противника?
14. Порядок моделирования и оценки вариантов действий.
15. Какие основные вопросы отражаются в решении на защиту информации?
16. Перечислите основные методы инженерно-технической защиты информации.

4 МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

В предыдущих главах были рассмотрены возможные технические каналы утечки информации из контролируемого помещения (объекта), а также была дана общая характеристика аппаратуры по обнаружению возможных каналов утечки. Большое количество технических каналов утечки информации обусловливает необходимость применения различных технических средств по их выявлению и борьбе с ними. Таким образом, объем работ по защите информации будет прежде всего зависеть от:

- оценки возможностей вероятного противника;
- стоящих перед организацией задач по защите;
- объема выделенных для работ по защите сил и средств;
- принятого руководителем организации решения на защиту информации.

Следовательно, рассмотрение основных методов и средств защиты информации целесообразно построить следующим образом:

- в первую очередь рассмотреть возможные варианты защиты наиболее подверженной утечке и менее защищенной от нее речевой информации;
- затем защиту информации, обрабатываемой техническими средствами;
- организацию защиты информации от утечки, возникающей при работе вычислительной техники, за счет ПЭМИН;
- организацию защиты ПЭВМ от несанкционированного доступа.

4.1. Организация защиты речевой информации

Не подлежит сомнению, что наивысшую ценность представляет информация, передаваемая устно. Это объясняется рядом специфических особенностей, свойственных речи. Устно сообщают сведения, которые не могут быть доверены техническим средствам передачи. Информация, полученная в момент ее озвучивания, является самой оперативной. Живая речь, несущая эмоциональную окраску личностного отношения к сообщению, позволяет составить психологический

портрет человека. Кроме того, современные методы дают возможность однозначно идентифицировать личность говорящего.

Этими особенностями и объясняется неослабевающий интерес противоборствующих сторон к непосредственному прослушиванию речи, циркулирующей в помещениях, по вибрационному и акустическому (воздуховоды, окна, потолки, трубопроводы) каналам. Поэтому вопросам защиты речевой информации уделяется первоочередное внимание при решении вопросов по защите от утечки информации по техническим каналам.

Существуют пассивные и активные способы защиты речи от несанкционированного прослушивания. Пассивные предполагают ослабление непосредственно акустических сигналов, циркулирующих в помещении, а также продуктов электроакустических преобразований в соединительных линиях ВТСС, возникающих как естественным путем, так и в результате ВЧ навязывания. Активные предусматривают создание маскирующих помех, подавление аппаратов звукозаписи и подслушивающих устройств, а также уничтожение последних.

Ослабление акустических сигналов осуществляется звукоизоляцией помещений. Прохождению информационных электрических сигналов и сигналов высокочастотного навязывания препятствуют фильтры. Активная защита реализуется различного рода генераторами помех, устройствами подавления и уничтожения.

4.1.1. Пассивные средства защиты выделенных помещений

Пассивные архитектурно-строительные средства защиты выделенных помещений. Основная идея пассивных средств защиты информации — это снижение отношения сигнал/шум в возможных точках перехвата информации за счет снижения уровня информативного сигнала.

При выборе ограждающих конструкций выделенных помещений в процессе проектирования необходимо руководствоваться следующими правилами:

- в качестве перекрытий рекомендуется использовать акустически неоднородные конструкции;
- в качестве полов целесообразно использовать конструкции на упругом основании или конструкции, установленные на виброизоляторы;
- потолки целесообразно выполнять подвесными, звукопоглощающими со звукоизолирующим слоем;
- в качестве стен и перегородок предпочтительно использование многослойных акустически неоднородных конструкций с упругими прокладками (резина, пробка, ДВП, МВП и т. п.).

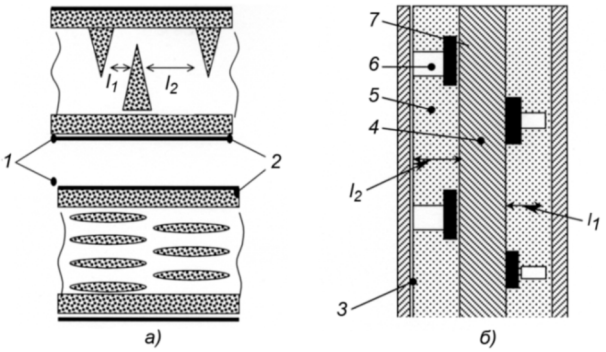


Рис. 4.1. Пассивные методы защиты короба вентиляции (*а*) и стены (*б*): *1* — стенки короба вентиляции; *2* — звукопоглощающий материал; *3*— отнесенная плита; *4* — несущая конструкция; *5* — звукопоглощающий материал;*6* — обрешетка; *7*— виброизолятор

Если стены и перегородки выполнены однослойными, акустически однородными, то их целесообразно усиливать конструкцией типа «стена на относе», устанавливаемой со стороны помещения.

Оконные стекла желательно виброизолировать от рам с помощью резиновых прокладок. Целесообразно применение двойного остекления окон двух- или трёхкамерным стеклопакетом на двух рамах, закрепленных на отдельных коробках. При этом между коробками укладывается звукопоглощающий материал.

В качестве дверей целесообразно использовать двойные двери с тамбуром, при этом дверные коробки должны иметь вибрационную развязку друг от друга.

Некоторые варианты технических решений пассивных методов защиты представлены на рис. 4.1.

Звукоизоляция помещений. Выделение акустического сигнала на фоне естественных шумов происходит при определенных отношениях сигнал/шум. Производя звукоизоляцию, добиваются его снижения до предела, затрудняющего (исключающего) возможность выделения речевых сигналов, проникающих за пределы контролируемой зоны по акустическому или вибрационному (ограждающие конструкции, трубопроводы) каналам.

Для сплошных однородных строительных конструкций ослабление акустического сигнала, характеризующее качество звукоизоляции на средних частотах, рассчитывается по формуле

$$K_{\text{ог}} = 20\lg(q_{\text{ог}} f) - 47{,}5 \text{ дБ},$$

где $q_{\text{ог}}$ — масса 1 м^2 ограждения, кг; f — частота звука, Гц.

Так как средний уровень громкости разговора, происходящего в

помещении, равен 50...60 дБ, звукоизоляция выделенных помещений в зависимости от присвоенных категорий должна быть не менее норм, приведенных в табл. 4.1. Самыми слабыми изолирующими качествами обладают двери (табл. 4.2) и окна (табл. 4.3).

Таблица 4.1

Звукоизоляция основных строительных конструкций, дБ

Частота, Гц	Категория помещения		
	1	2	3
500	53	48	43
1000	56	51	46
2000	56	51	46
4000	55	50	45

Во временно используемых помещениях применяют складные экраны, эффективность которых с учетом дифракции составляет от 8 до 10 дБ. Применение звукопоглощающих материалов для преобразования кинетической энергии звуковой волны в тепловую энергию имеет некоторые особенности. Они связаны с необходимостью создания оптимального соотношения прямого и отраженного от преграды акустических сигналов. Чрезмерное звукопоглощение снижает уровень сигнала, а большое время реверберации приводит к ухудшению разборчивости речи. Ослабления звука ограждениями, выполненными из различных материалов, приведены в табл. 4.4.

Таблица 4.2

Конструкция	Звукоизоляция, дБ, на частотах, Гц					
	125	250	500	1000	2000	4000
Щитовая дверь, облицованная фанерой с двух сторон:						
без прокладки	21	23	24	24	24	23
с прокладкой из пористой резины	27	27	32	35	34	35
Типовая дверь П-327:						
без прокладки	13	23	31	33	34	36
с прокладкой из пористой резины	29	30	31	33	34	41

Таблица 4.3

Схема остекления	Звукоизоляция, дБ, на частотах, Гц					
	125	250	500	1000	2000	4000
Одинарное остекление:						
толщина 3 мм	17	17	22	28	31	32
толщина 4 мм	18	23	26	31	32	32
толщина 6 мм	22	22	26	30	27	25
Двойное остекление с воздушным промежутком:						
57 мм (толщина 3 мм)	15	20	32	41	49	46
90 мм (толщина 3 мм)	21	29	38	44	50	48
57 мм (толщина 4 мм)	21	31	38	46	49	35
90 мм (толщина 4 мм)	25	33	41	47	48	36

Таблица 4.4

Тип ограждения	Коэффициент поглощения $K_{\text{ог}}$ на частотах, Гц					
	125	250	500	1000	2000	4000
Кирпичная стена	0,024	0,025	0,032	0,041	0,049	0,07
Деревянная обивка	0,1	0,11	0,11	0,08	0,082	0,11
Стекло одинарное	0,03	*	0,027	*	0,02	*
Штукатурка известковая	0,025	0,04	0,06	0,085	0,043	0,058
Войлок (толщина 25 мм)	0,18	0,36	0,71	0,8	0,82	0,85
Ковер с ворсом	0,09	0,08	0,21	0,27	0,27	0,37
Стеклянная вата (толщиной 9 мм)	0,32	0,4	0,51	0,6	0,65	0,6
Хлопчатобумажная ткань	0,03	0,04	0,11	0,17	0,24	0,35

Уровень сигнала за преградой $R_{\text{ог}}$, дБ, оценивается выражением

$$R_{\text{ог}} = R_c + 6 + 10 \lg S_{\text{ог}} - K_{\text{ог}},$$

где $R_{\text{с}}$ — уровень речевого сигнала в помещении, дБ; $S_{\text{ог}}$ — площадь ограждения, м^2; $K_{\text{ог}}$ — коэффициент поглощения материала ограждения, дБ.

Звукоизолирующие кабины каркасного типа обеспечивают ослабление до 40 дБ, бескаркасного — до 55 дБ.

4.1.2. Аппаратура и способы активной защиты помещений от утечки речевой информации

Эффективность системы защиты оценивают превышением интенсивности маскирующего воздействия над уровнем акустических сигналов в воздушной или твердой средах. Величина превышения помехи над сигналом регламентируется руководящими документами ФСТЭК России.

Для защиты помещений применяют системы акустического и вибрационного зашумления состоящие из генераторов «белого» шума, малогабаритных колонок, вибровозбудителей электромагнитного и (или) пьезоэлектрического принципа действия.

Так, в комплекте системы вибрационной и акустической защиты ANG-2000 поставляется акустический излучатель (колонка) OMS-2000. В различных системах применяются акустические излучатели, отличающиеся габаритами, мощностью и другими характеристиками, такие как АИ-3М, АИ-65, СА-65М, СТД-А, OMS2000 и АСМик-1. Однако применение динамиков создает не только маскирующий эффект, но и помехи нормальной повседневной работе персонала в защищаемом помещении.

Эффективность систем и устройств вибрационного зашумления определяется и свойствами применяемых электроакустических преобразователей (вибровозбудителей), трансформирующих электрические колебания в упругие колебания (вибрации) твердых сред. Качес-

тво преобразования зависит от реализуемого физического принципа, конструктивно-технологического решения и условий согласования вибропреобразователя со средой.

Как было отмечено, источники маскирующих воздействий должны, как минимум, иметь частотный диапазон, соответствующий ширине спектра речевого сигнала (200...5000 Гц). Следовательно, особую важность приобретает выполнение условий согласования преобразователя с конструкцией в широкой полосе частот. Условия широкополосного согласования с ограждающими конструкциями, имеющими высокое акустическое сопротивление (кирпичная стена, бетонное перекрытие), наилучшим образом выполняются при использовании вибродатчиков с высоким механическим импедансом подвижной части. Такими датчиками, на сегодняшний день, являются пьезокерамические вибровозбудители.

Во время работы вибровозбудителей также возникают паразитные акустические шумы, вносящие дискомфорт и нарушающие нормальные условия труда в защищаемом помещении. В зависимости от механизма образования различают акустические шумы, переизлученные твердой средой, и звуковые колебания, генерируемые собственно преобразователем (его корпусом). В этом случае соотношение акустических сопротивлений

$$\gamma = \rho_1 c_1 / \rho_2 c_2,$$

где ρ_1, ρ_2 — плотность, кг/м^3, а c_1, c_2 — скорости звука, м/с, в твердой среде и воздухе соответственно. Как следует из этого соотношения, в силу большой разницы акустических сопротивлений уровень шумов, переизлученных средой в воздух, весьма незначителен, поэтому основным источником паразитных акустических шумов является вибровозбудитель. На рис. 4.2 приведены амплитудно-частотные характеристики акустических помех, создаваемых при работе систем вибрационного зашумления.

Монтаж вибровозбудителей, как правило, сопряжен с необходимостью выполнения трудоемких строительно-монтажных работ — сверлением, установкой дюбелей, выравниванием поверхностей, приклеиванием и т. п.

Оригинальная методика крепления (рис. 4.3) вибровозбудителей, реализованная в мобильной системе «Фон-В», позволяет значительно расширить диапазон применения генератора ANG-2000 и преобразователей TRN-2000.

Два комплекта металлических стоек позволяют оперативно установить вибродатчики в неподготовленных помещениях площадью до 25 м^2. Монтаж и демонтаж конструкций и датчиков осуществляется

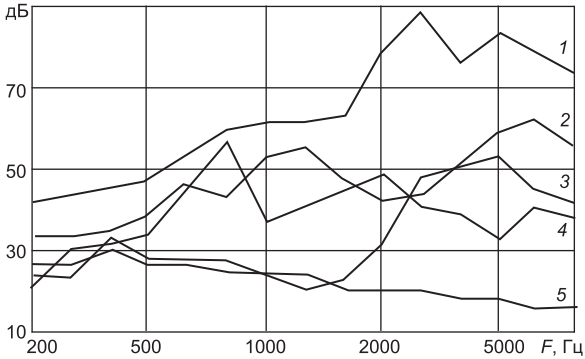


Рис. 4.2. Амплитудно-частотные характеристики акустических помех: *1* — ANG-2000 + TRN-2000; *2* — VNG-006DM; *3* — VNG-006 (1997 г.); *4* — «Заслон-АМ» и «Порог-2М»; *5* — фоновые акустические шумы помещения

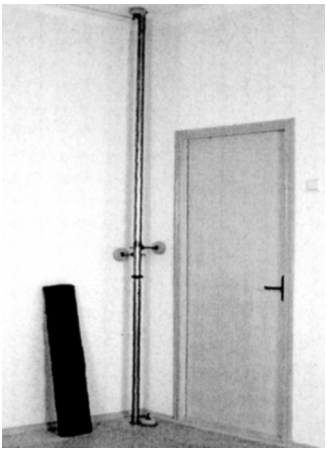


Рис. 4.3. Мобильная система «Фон-В»

в течение 30 мин силами трех человек без повреждений ограждающих конструкций и элементов отделки интерьера.

Ввиду частотной зависимости акустического сопротивления материальных сред и конструктивных особенностей вибровозбудителей на различных частотах необходимо создавать весьма различные уровни виброшума. Поэтому применение систем зашумления без гибкой частотной регулировки вынуждает увеличивать общий уровень мощности, подводимый к вибровозбудителям.

Увеличение мощности помехи создает повышение уровня паразитного акустического шума, что вызывает дискомфорт у работающих в помещении людей. Это приводит к отключению системы в наиболее ответственные моменты, создавая предпосылки к утечке конфиденциальных сведений.

В то же время системы с наличием таких регулировок, с большим числом независимо регулируемых каналов позволяют оптимально настроить систему защиты с минимально необходимыми в каждой октавной полосе отношением сигнал/шум, резко снижая уровень паразитных шумов в помещении.

Оптимальные параметры помех. В случае применения активных средств необходимое для обеспечения защиты информации отношение сигнал/шум достигается за счет увеличения уровня шумов в воз-

можных точках перехвата информации при помощи генерации искусственных акустических и вибрационных помех. Частотный диапазон помехи должен соответствовать среднестатистическому спектру речи в соответствии с требованиями руководящих документов.

В связи с тем, что речь — шумоподобный процесс со сложной (в общем случае случайной) амплитудной и частотной модуляциями, наилучшей формой маскирующего помехового сигнала является шумовой процесс с нормальным законом распределения плотности вероятности мгновенных значений (т. е. белый или розовый шум). Именно эта концепция является основой действующих требований к защите речевой информации.

Спектр помехи в общем случае должен соответствовать спектру маскирующего сигнала, но с учетом того, что информационная насыщенность различных участков спектра информативного сигнала не одинакова, для каждой октавной полосы установлена своя величина превышения помехи над сигналом. Нормированные отношения сигнал/шум в октавных полосах для каждой категории выделенных помещений приводятся в руководящих документах. Такой дифференцированный подход к формированию спектра помехи позволяет минимизировать энергию помехи, снизить уровень паразитных акустических шумов при выполнении норм защиты информации. Сформированная таким образом помеха является оптимальной.

Рассматривая вопросы о создании оптимальных помех, необходимо отметить, что разрабатываемые системы должны обеспечить защиту от следующих технических средств съема информации:

- устройств, использующих контактные микрофоны (электронных проводных и беспроводных акселерометрических и тензометрических контактных микрофонов);
- устройств дистанционного съема информации (лазерные микрофоны, направленные микрофоны);
- закладочных устройств, внедряемых в элементы строительных конструкций.

Кроме того, они должны защищать:

- внешние и внутренние стены жесткости, выполненные из монолитного железобетона, железобетонных панелей и кирпичной кладки толщиной до 500 мм;
- плиты перекрытий, в том числе и покрытые слоем отсыпки и стяжки;
- внутренние перегородки из различных материалов;
- остекленные оконные проемы;
- трубы отопления, водоснабжения, электропроводки;
- короба систем вентиляции, тамбуры.

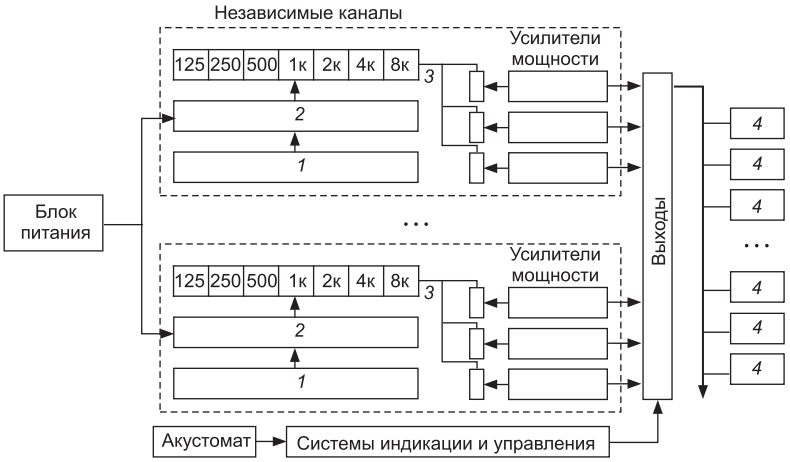


Рис. 4.4. Структурная схема системы активной защиты речевой информации: *1* — генератор белого шума; *2* — полосовой фильтр; *3* — октавный эквалайзер с центральными частотами 125, 250, 500, 1000, 2000, 4000 и 8000 Гц; *4* — преобразователи (акустические колонки, вибровозбудители)

Такие задачи в настоящее время решает большинство из представленных на российском рынке систем постановки вибрационных и акустических помех, таких как системы семейств «Соната-АВ» (моделей 1М, 2М, 3М, 2Б), «Шорох» (моделей 1М, 2М, 3 и 4), «Шторм» (моделей 2, 5, 7), SEL SP-55 (моделей 2, 4), «Барон», «Кедр», «Октава-ВА» и др.

Следует отметить, что каждое помещение и каждый элемент строительной конструкции имеют свои индивидуальные амплитудно-частотные характеристики распространения колебаний. Поэтому при распространении форма спектра первичного речевого сигнала изменяется в соответствии с передаточной характеристикой траектории распространения. В этих условиях для создания оптимальной помехи необходима корректировка формы спектра помехи в соответствии со спектром информативного сигнала в точке возможного перехвата информации.

Структурная схема системы, оптимально реализующей активные методы защиты речевой информации, соответствующие требованиям руководящих документов, приведена на рис. 4.4.

Рис. 4.5. Общий вид генератора SEL SP-55/4

Генератор SEL SP-55/4 (рис. 4.5). Основные узлы генератора — формирователи шума, эквалайзеры и выходные усилители представляют собой цифровые устройства. Это позволяет проще решить ряд задач.

Рис. 4.6. Общий вид и структурные элементы системы «Шторм-5»

Диапазон частот 0,1...5,6 кГц. Номинальная (при линейной АЧХ) выходная мощность по одному каналу при нагрузке 4 Ом равна 2,5 Вт. Диапазон регулирования уровня в каждой октавной полосе эквалайзера по любому каналу не менее 5 дБ. Количество каналов генератора SEL SP-55/4 — 4. Количество излучателей, подключаемых на один канал, до 12. Продолжительность непрерывной работы не менее 8 часов.

Наличие независимых пятиполосных эквалайзеров для каждого канала позволяет оптимизировать спектр помехи для получения минимального побочного акустического шума в защищаемом помещении. Каждый канал имеет независимую защиту от перегрузки и короткого замыкания. Во время работы прибор постоянно контролирует исправность нагрузки каждого канала и в случае её неисправности — обрыве или замыкании одного или нескольких виброизлучателей или колонок — выдает звуковой и световой сигналы.

«Шторм-5» (рис. 4.6). В состав системы входят: трехканальный прибор вибрационной и акустической защиты SI-3030; электромагнитные вибровозбудители TRN-2000; вибровозбудители ВД-1; акустические излучатели OMS-2000. Шумогенератор SI-3030 имеет три независимых канала и допускает подключение вибрационных и акустических излучателей отечественного и импортного производства любого типа. В приборе используются три некоррелированные источника шума. Независимая регулировка уровня выходного сигнала в каждом канале позволяет настраивать прибор с разными типами датчиков под конкретные условия эксплуатации. Возможна корректировка АЧХ спектра выходного сигнала в каждом канале. Благодаря возможности подключения любых типов вибрационных и акустических излучателей потребитель может модифицировать имеющуюся систему защиты без

демонтажа и замены ранее установленных излучателей. Прибор имеет высокий КПД, обладает большой выходной мощностью благодаря новым техническим решениям.

Рис. 4.7. Генератор «Барон»

Система «Барон» (рис. 4.7) имеет четырёхканальное построение системы при мощности каждого канала не менее 18 Вт. В каждом канале пятиполосный эквалайзер. Диапазон частот 60...16000 Гц. Частотные поддиапазоны с регулированием уровня помехи 60...350 Гц; 350...700 Гц; 700...1400 Гц; 1400...2800 Гц; 2800...16000 Гц. В каждом канале независимые генераторы шума. Диапазон регулировки уровня сигнала в каждой октавной полосе не менее 24 дБ. Система имеет полностью цифровое управление, интеллектуальное меню и гибкую систему конфигурирования. Кроме того, наличие линейного входа позволяет подключать к комплексу источники специального помехового сигнала повышенной эффективности.

В соответствии с такой структурной схемой построены системы постановки вибрационных и акустических помех семейства «Шорох».

Рассмотрим основные характеристики современных систем постановки вибрационных и акустических помех.

«Шорох-3» (рис. 4.8). Система построена по модульному принципу. Каждый модуль имеет 2 независимых канала. В качестве помехи генерируется аналоговый шум с нормальным распределением плот-

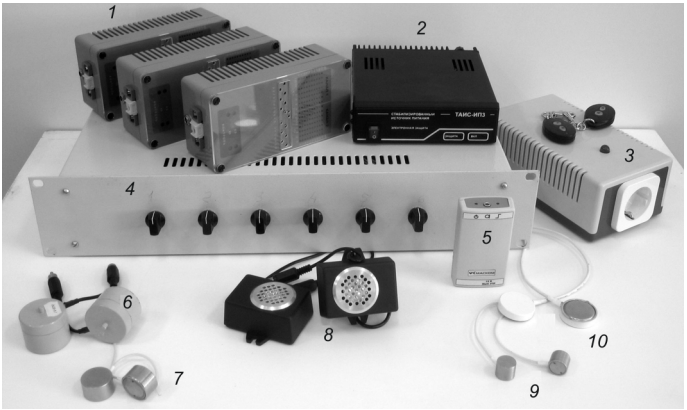


Рис. 4.8. Общий вид основных составляющих частей системы «Шорох-3»: *1* — блоки ГШВА-2; *2* — блок питания ТАИС-ИП3; *3* — «Шорох-ДУ; *4* — блок УС-6; *5* — устройство ГУ; *6* — преобразователи КВП-2; *7* — преобразователи ПЭД-5; *8* — преобразователи АСМик-1; *9* — преобразователи ПЭД-5; *10* — преобразователи КВП-7

ности вероятности мгновенных значений и гарантированным коэффициентом качества. Действующее значение напряжения помехи не менее 4 В, с устройством УС-6 — не менее 30 В. Помеха генерируется в диапазоне частот 157...11200 Гц. Спектральные характеристики генерируемой помехи регулируются шестиполосным октавным эквалайзером с центральными частотами 250, 500, 1000, 2000, 4000, 8000 Гц. Глубина регулировки спектра по полосам не менее 27 дБ и общего уровня помехи не менее 40 дБ.

Общее количество одновременно подключаемых электроакустических преобразователей на один канал: 4–6 КВП-2, КВП-7; 4–6 ПЭД-5,6; 1–4 акустических колонок (4...8 Ом). Выходная мощность канала не менее 3 Вт. Габариты модуля 165×80×60 мм. Вес модуля не более 450 г.

«Шорох-4» (рис. 4.9). Система построена по блочно-модульному принципу. Каждый модуль имеет 1 или 2 независимых канала. В качестве помехи генерируется аналоговый шум с нормальным распределением плотности вероятности мгновенных значений и гарантированным коэффициентом качества (не ниже 0,93). Действующее значение напряжения помехи — не менее 10 или 18 В. Помеха генерируется в диапазоне частот 100...12500 Гц. Спектральные характеристики генерируемой помехи регулируются семиполосным октавным эквалайзером в центральных частотах 125, 250, 500, 1000, 2000, 4000, 8000 Гц полос регулировки спектра. Глубина регулировки спектра и уровня помехи по полосам не менее 32 дБ.

Рис. 4.9. Общий вид основных составляющих системы «Шорох-4»

Общее количество одновременно подключаемых электроакустических преобразователей на один канал: 4–6 КВП-2, КВП-7; 4–6 ПЭД-5,6; 1–4 акустических колонок (4...8 Ом). Выходная мощность канала не менее 3 Вт. Габариты модуля 165×80×60 мм. Масса блока с 4-я модулями не более 4,5 кг. Уникальными особенностями системы являются:

- исключение возможности несанкционированного изменения настроек системы;
- возможность «горячей» замены любого модуля без перенастройки системы;
- интеллектуальная многоточечная система самоконтроля работоспособности электропитания, канала и нагрузки.

Адаптивный генератор помехи «Кедр» (рис. 4.10) анализирует акустическую обстановку в помещении и на основании результатов

Рис. 4.10. Адаптивный генератор вибрационной и акустической помех «Кедр»

Рис. 4.11. Генератор «Соната-АВ» мод. 3Б

анализа, по встроенному алгоритму, формирует сигнал управления, функционально связанный с огибающей акустического (речевого) сигнала. Сформированный сигнал управляет параметрами генератора шума на основе 64 разрядной двоичной псевдослучайной последовательности, как во временной области, так и по амплитуде. Это позволяет локализовать помеху во время произнесения слов и повысить ее спектральную плотность. Полоса частот сигнала защиты 200 Гц... ...15 кГц. Количество каналов 3. Максимальное количество виброизлучателей, подключаемых на 1-й и 2-й канал, 20. Максимальное количество акустоизлучателей 4. Радиус действия одного вибродатчика 1,5 м. Количество подключаемых микрофонов 2. Минимальное сопротивление акустоизлучателей 4 Ом.

Прибор может работать в двух режимах: адаптивный и непрерывный. При работе в адаптивном режиме обеспечивается оптимальное перекрытие уровня речи уровнем помехи в строительных конструкциях, а также минимальное излучение шума в само помещение. В каждом канале генератора имеется цифровой 7-полосный графический эквалайзер, позволяющий проводить настройку канала под конкретные условия (стена, окно и т. п.) и различные виды вибродатчиков. Наличие встроенный памяти позволяет запоминать до 16 вариантов амплитудно-частотных характеристик эквайлайзера (по 4 на каждый канал). Система акустопуска и наличие ДУ (проводного или по радиоканалу) дает возможность осуществлять гибкое управление процессом генерации помехи.

«Соната-АВ» модель 3Б (рис. 4.11). Системным признаком модели 3Б аппаратуры «Соната-АВ» является построение по принципу «единый источник электропитания + генераторы-излучатели». Система состоит из генераторов-излучателей СВ-45М, СП-45М, генераторов-аудиоизлучателей СА-65М, которые совместно с источником питания образуют систему генераторов-преобразователей, т. е. каждый преобразователь — независимый канал. Задатчики сигнала цифровые. Полоса воспроизводимых частот 175...5600 Гц. Максималь-

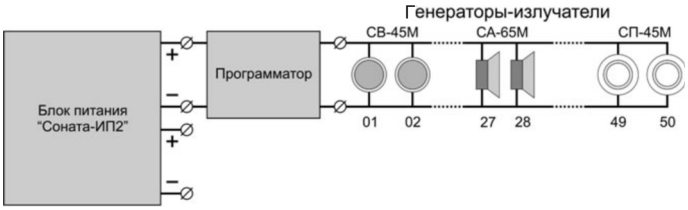


Рис. 4.12. Принципиальная схема системы «Соната-АВ» мод. 3М

ный ток потребления не более 20 мА. Максимальное число индивидуальных адресов 255.

Корректировка интегрального уровня и спектра шума, создаваемого изделиями СВ-45М, СП-45М и СА-65М, осуществляется при помощи либо ручного («Соната-ПРГ1»), либо компьютерного («Соната-ПРГ2») программатора, включаемого на время настройки, как указано на рис. 4.12. Параметры установки сохраняются в энергонезависимой памяти. Во время программирования обращения к генераторам-излучателям осуществляется адресно и остальные изделия системы могут не отключаться от линии электропитания. По умолчанию всем изделиям присваивается адрес 01. Установка адреса в пределах от 01 до 99 может быть выполнена при помощи программаторов. Программаторы используются только при настройке системы, после чего отключаются.

Рассматривая вопросы организации защиты информации, мы неоднократно говорили о том, что защита информации в современных условиях невозможна без комплексного подхода, без организации системы защиты. Прежде всего, это обусловлено многообразием объектов защиты, различными условиями эксплуатации как средств обработки, так и средств защиты информации, а также меняющимися во времени требованиями к конкретным объектам и возможностями организаций и предприятий по обеспечению режимных подразделений средствами защиты информации.

Комплексный подход к организации системы защиты должен позволять решать следующие задачи:

- создание простых и недорогих систем защиты информации с возможностью дальнейшего их расширения не только в количественном, но и в качественном смысле;
- минимизация расходов на проектирование и инсталляцию систем защиты информации;
- гибкое изменение и/или наращивание функциональных возможностей уже имеющихся систем защиты информации;
- комфортное оперативное управление;
- возможность включения в систему технических средств разных

производителей и даже не имеющих входа дистанционного управления (блокираторы мобильной связи, блокираторы диктофонов и др.);
- мониторинг режима работы и исправности входящих в состав системы устройств;
- исключение возможности негативного взаимного влияния устройств защиты информации и других технических средств.

В настоящее время решение этих задач стало возможно с применением полнофункционального автоматизированного комплекса технических средств защиты информации от утечки по техническим каналам «Унисон-АВР» (рис. 4.13).

Базовым элементом комплекса является устройство «Соната-ИП3» (блок питания, управления и программирования). Для повышения универсальности комплекса разработан ряд устройств дистанционного управления:
- транслятор команд «Соната-ДУ21М», который подключается к двухпроводному кабелю и обеспечивает связь между устройством «Соната-Рх» и блоком «Соната-ИП3» по ИК каналу;
- точка доступа «Соната-ДУ21М», который также подключается к двухпроводному кабелю и принимает сигналы от ИК пульта (включение выключение системы), может располагаться в любом месте защищаемого помещения;
- транслятор команд «Соната-ДУ21М», подключаемый к двухпроводному кабелю и обеспечивающий связь между устройствами «Соната-РСх», «Соната-ДУ-К2» и блоком «Соната-ИП3» по ИК каналу.

Автоматизированный комплекс «Унисон-АВР» обеспечивает защиту от утечки за счет акустоэлектрических преобразований. Устройство «Соната-ВК» обеспечивают физический разрыв слаботочных линий и конструктивно выполнено в трех модификациях.

Модель ВК1 предназначена для защиты абонентских телефонных аппаратов. Особенность модели состоит в том, что при появлении вызывного сигнала в линии устройство умеет оповещать об этом звуковым сигналом.

Модель ВК2 предназначена для защиты речевой информации от утечки через линии системы оповещения и системы охранной сигнализации.

Модель ВК3 предназначена для защиты от утечки по линиям Ethernet.

Особенность устройств «Соната-ВК» — это возможность интеграции в систему виброакустической защиты «Соната-АВ» модель 3Б.

Кроме того, защита от утечки за счет ПЭМИН обеспечивается использованием аппаратуры серии «Соната-Рхх» и клавиатур в за-

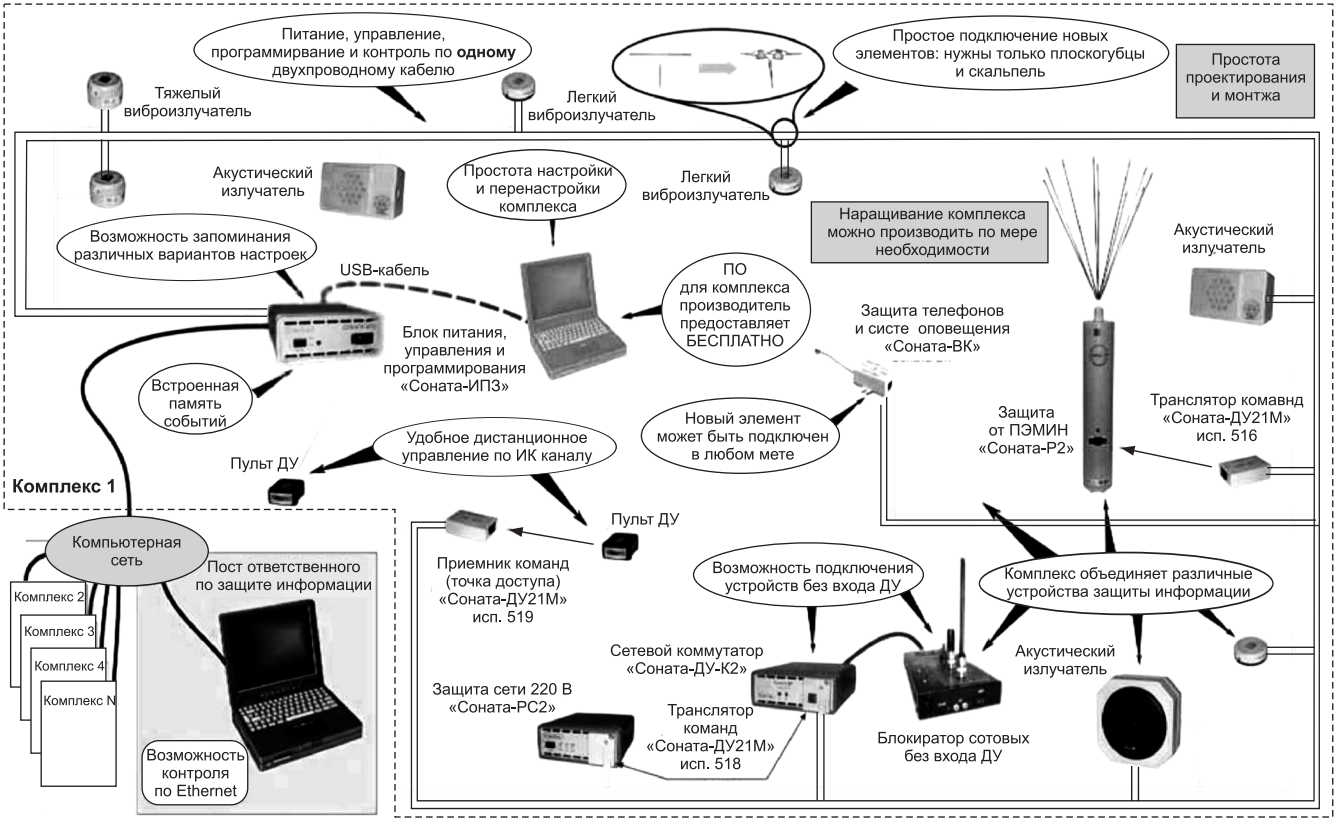


Рис. 4.13. Структурная схема автоматизированного комплекса «Унисон-АВР»

щищенном исполнении «Фарватер-КВ1», которые не позволяют совершить перехват вводимой с них информации по побочным электромагнитным излучениям. В технических решениях использованных в данной клавиатуре реализован запатентованный способ защиты информации, который предотвращает даже теоретическую возможность перехвата вводимой информации.

Производство клавиатуры, так же как и генераторов, сертифицировано ФСТЭК России для применения на объектах вычислительной техники, в том числе обрабатывающих секретную информацию.

Рассмотрение вопросов защиты помещений от утечки различных видов информации связано прежде всего с конструктивными особенностями защищаемых помещений, что вызывает необходимость рассмотрения этих особенностей.

Особенности постановки акустических помех. Основную опасность с точки зрения возможности утечки информации по акустическому каналу представляют различные звуководы — строительные тоннели и короба, предназначенные для осуществления вентиляции и размещения различных коммуникаций. Контрольные точки при оценке защищенности таких конструкций выбираются непосредственно на границе их выхода в выделенное помещение или в точках их выхода в ближайшие смежные помещения. Акустические излучатели системы постановки помех размещаются в объеме короба на таком расстоянии от выходного отверстия, чтобы акустический шум минимально проникал в помещение.

Дверные проемы, в том числе оборудованные тамбурами, также являются источниками повышенной опасности и в случае недостаточной звукоизоляции также нуждаются в применении активных методов защиты. Акустические излучатели систем зашумления в этом случае желательно располагать снаружи тамбура, вблизи дверной коробки со стороны смежного помещения. При таком размещении колонок системы зашумления (САЗ) «просачивающийся сигнал» имеет наименьшую величину, для его зашумления нужна минимальная мощность шума, как правило, уже не мешающая персоналу. А в защищаемое помещение шум вообще не проникает. Контроль выполнения норм защиты информации в этом случае проводится вблизи внешней поверхности внешней (по отношению к защищаемому помещению) двери тамбура.

Более подробно эти вопросы будут рассмотрены в главе, посвящённой проведению специальных исследований.

Особенности постановки вибрационных помех. Несмотря на то что некоторые системы постановки вибрационных помех обладают достаточно мощными генераторами и эффективными вибровозбудителями, обеспечивающими значительные радиусы действия, критери-

ем выбора количества преобразователей и мест их установки должны быть не максимальные возможные значения параметров систем, а конкретные условия их эксплуатации.

Так, например, если здание, в котором находится выделенное помещение, выполнено из сборного железобетона, вибровозбудители системы зашумления должны располагаться на каждом элементе строительной конструкции, несмотря на то что в процессе оборудования помещения измерения могут показать, что одного преобразователя достаточно для зашумления нескольких элементов (нескольких плит перекрытия или нескольких стеновых панелей). Необходимость такой методики установки преобразователей продиктована отсутствием временно́й стабильности акустической проводимости в стыках строительных конструкций. В пределах каждого элемента строительной конструкции предпочтительно выбирать места установки преобразователей в области геометрического центра этого элемента.

Следует отметить особую важность технологии крепления преобразователя к строительной конструкции. В акустическом плане крепежные приспособления являются согласующими элементами между источниками излучения — преобразователями и средой, в которой это излучение распространяется, т. е. строительной конструкцией. Поэтому крепежное устройство (помимо того, что оно должно быть точно рассчитано) должно не только прочно держаться в стене, но и обеспечивать полный акустический контакт своей поверхности с материалом строительной конструкции. Это достигается исключением щелей и зазоров в узле крепления с помощью клеев и вяжущих материалов с минимальными коэффициентами усадки и малыми декрементами затухания.

Важным параметром, характеризующим работу системы постановки вибрационных и акустических помех, является уровень паразитных акустических шумов, излучаемых в объем выделенного помещения. Эти шумы генерируются двумя источниками.

Во-первых, это вибрация защищаемых строительных конструкций. В общем случае, если создана оптимальная вибрационная помеха, эти шумы не зависят от системы зашумления и могут быть минимизированы только увеличением равномерности плотности энергии помехи в плоскости защищаемой конструкции за счет увеличения количества преобразователей.

Во-вторых, источником акустических шумов является собственно работающий преобразователь. Акустическое излучение вибровозбудителей можно существенно снизить, размещая их в заранее подготовленных в строительных конструкциях нишах, закрытых, например, штукатуркой после установки преобразователя. Более простым, но

не менее эффективным способом снижения уровня паразитных акустических шумов является применение акустических экранов. Экран представляет собой легкую жесткую конструкцию, отделяющую преобразователь от объема выделенного помещения. Схема установки вибровозбудителя и акустического экрана рассмотрена в разд. 5.2.4 (рис. 5.43), а эффективность действия экранов показана на рис. 4.14.

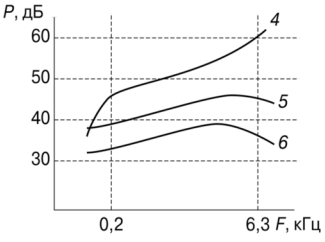


Рис. 4.14. Эффективность действия экранов

Из рис. 4.14 видно, что применение экрана снижает акустическое излучение преобразователя на 5...17 дБ, причем наибольший эффект достигается в области средних и высоких частот, т. е. в области наибольшей слышимости. Экран следует устанавливать таким образом, чтобы его внутренняя поверхность не соприкасалась с корпусом преобразователя и в местах прилегания экрана к строительной конструкции отсутствовали щели и неплотности.

4.1.3. Рекомендации по выбору систем вибрационной и акустической защиты

В настоящее время на рынке средств защиты информации системы вибрационного и акустического зашумления представлены достаточно широко, и интерес к ним не спадает.

Следует отметить, что корректное сопоставление параметров различных систем только на основании данных фирм-производителей невозможно из-за различия теоретических концепций, методик измерения параметров, условий производства.

В настоящее время основным критерием выбора систем защиты можно считать стоимость решения. При этом в понятие стоимости решения нужно включать не только стоимость реализации, но и стоимость эксплуатации, контроля эффективности, ремонта и т. д.

Как правило, пассивная система защиты обеспечивает более комфортные условия для работников в ходе эксплуатации объектов, но строительные решения, как правило, заметно дороже у активных систем (зашумления). Однако при рассмотрении вопросов эксплуатации хотя бы в течение первого десятка лет с учётом необходимости ежегодных расходов на ремонт, периодический инструментальный контроль, замену средств, у которых окончилось действие сертификата, и т. д. общие стоимости пассивного и активного вариантов защиты разнятся уже не очень сильно.

Кроме того, мы уже говорили о том, что пассивные меры защиты ничем не нарушают комфортность рабочих помещений. Наоборот, уровень шумов в таких помещениях заметно меньше, чем в

незащищённых. Активные же решения неизбежно ухудшают комфортность помещений за счёт паразитного шума от всех преобразователей. Пренебрежение этим фактором, неоптимальное построение систем зашумления, их непрофессиональная, неаккуратная настройка настолько ухудшают условия нахождения в помещении, что систему защиты просто выключают.

Поэтому, рассматривая особенности построения системы активной защиты различных помещений, необходимо рассматривать каждое защищаемое помещение отдельно. При этом особое внимание необходимо обратить на структуру ограждающих конструкций. Как не странно, но зашумление облегчённых ограждающих конструкций типа лёгких перегородок, выполненных из материалов класса гипсокартона или МДВ, является наиболее проблематичным. Данные ограничивающие конструкции по отношении к акустической волне являются эффективной мембраной, а вот зашумляющий сигнал от точки размещения вибровозбудителя распространяется внутри такого листа с большим затуханием. Это приводит к необходимости установки значительного количества вибровозбудителей на единицу площади, что приводит к экономической нецелесообразности именно активных методов защиты. Такие перегородки целесообразно изначально проектировать в защищенном исполнении, обеспечивающем защиту от утечки по акустическому и вибрационному каналам пассивными методами. Необходимо отметить, что в настоящее время в наличии широкий спектр специализированных материалов и применение их для организации пассивной защиты незначительно увеличивает стоимость работ.

Ограничивающие конструкции в капитальном исполнении (кирпичная кладка от 250 мм, сборный и монолитный бетон, блочные конструкции) при отсутствии в них щелей, трещин и т. д. в большинстве случаев автоматически обеспечивают защищённость по акустическому каналу. По вибрационному каналу защиту пассивными методами могут обеспечить только специализированные многослойные конструкции типа «стена на относе». Типовые строительные решения обязательно требуют применения средств активной защиты. Именно этот вариант, как правило, оказывается наиболее экономически выгодным.

Более сложные элементы ограничивающих конструкций — окна и дверные проёмы. Обеспечить их защиту по акустическому каналу пассивными мерами можно только специальным конструированием и исполнением дверных и оконных проемов и специальных вариантов остекления. В ряде случаев это необходимо, но стоимость такого решения многократно превышает стоимость типовых строительных вариантов. По виброканалу окна (остекление) и дверные полотна могут быть защищены в большинстве случаев только активными мерами.

Однако в последнее время разработаны решения, базирующиеся на типовых строительных элементах, которые при не столь значительном удорожании обеспечивают защиту помещений чисто пассивными мерами.

В отношении систем вентиляции, кондиционирования, тепло- и водоснабжения стоимость пассивных и активных вариантов защиты различаются весьма значительно. Зашумление этих систем, как правило, несложно, хотя и требует весьма внимательного подхода к размещению вибровозбудителей и колонок.

Таким образом, проведенный анализ позволят сделать вывод, что основными критериями, которые определяют выбор между пассивной и активной защитой, должны быть:

- безусловное выполнение требований защищённости в любой точке окружающего пространства и конструкций помещений;
- минимизация стоимостных параметров системы защиты, её обслуживания, эксплуатации и контроля эффективности;
- выполнение действующих требований по шуму в помещениях (в соответствии с «Санитарными нормами допустимого шума в помещениях жилых и общественных зданий и на территории жилой застройки» и СНиП 23-03-2003, раздел 6 «Нормы допустимого шума»);
- выполнение требований по сохранению дизайна и комфортности помещений.

Считая, что данных рекомендаций достаточно для ориентировочного выбора системы защиты по стоимостным критериям, далее более детально рассмотрим особенности разнообразных систем активной защиты. Не касаясь довольно большого ряда средств активной защиты, которые направлены на обеспечение защищённости переговоров ограниченного числа лиц или локальной области пространства, будем рассматривать средства защиты стационарных защищаемых (выделенных) помещений.

При этом особое внимание необходимо обратить на то, что существующие основополагающие документы по данной проблеме рассматривают в качестве параметра защищённости отношение сигнал/шум (и некоторые другие параметры, вытекающие из этого отношения). В документах в качестве шума рассматривается только «белый» шум, т. е. шумовой сигнал, плотность распределения вероятности мгновенных значений которого подчиняется распределению Гаусса.

На этом основании все другие виды зашумляющего сигнала, такие как «речеподобная» помеха любых способов генерации, смеси различных сигналов и т. д., так же как и утверждения их защитников об их большой эффективности, можно отнести к чисто рекламным утверждениям, которые к тому же и вводят в заблуждение потребителя.

Такое положение сохранится до тех пор, пока регламентирующими документами не будут установлены иные параметры зашумляющего сигнала.

Основными элементами системы активной защиты, определяющими качество создаваемых акустического и вибрационного сигналов, являются задающий генератор, который формирует амплитудно-частотные характеристики, электроакустические преобразователи (колонки) и вибровозбудители.

Раэберемся в том, что же необходимо для разумного выбора системы зашумления.

В генераторах шумозвукового диапазона частот, как правило, используются в качестве задающего элемента шумовые диоды (шумы пробоя p-n-перехода). Не вдаваясь в особые детали, необходимо отметить, что данный шумовой сигнал в полной мере отвечает требованиям нормативных документов. В последнее время появилось достаточное количество генераторов шума с цифровым формирователем псевдослучайной последовательности. Генераторы этого типа обладают неотъемлемым свойством повторяемости псевдошумового сигнала во времени. То есть через некий промежуток времени вся последовательность псевдошумового сигнала начинает полностью повторяться.

В настоящее время отсутствуют утверждённые требования к такого рода цифровым генераторам псевдослучайных сигналов, как и требования к минимальным периодам повторяемости. Этот вопрос ещё подлежит рассмотрению и последующему формированию регламентирующих требований. Стоит только отметить, что уже сейчас свободно продаются средства цифровой записи речевого диапазона частот с надлежащим качеством, которые могут быть применены для перехвата (для целей последующей компенсации псевдошумового сигнала) в миниатюрном варианте с автономным электропитанием и временем непрерывной записи до 1000 часов.

Что касается узлов формирования АЧХ систем вибрационной и акустической защиты, то это важнейший их элемент. Чем более широкий диапазон регулировки в распоряжении пользователя, чем точнее с их помощью может быть выполнена настройка в каждой октавной полосе, тем более низкий уровень паразитных шумов может быть достигнут. Отсутствие многополосной регулировки (эквалайзера) должно рассматриваться как весьма серьёзный недостаток системы.

Напрямую к рассматриваемому свойству относятся и вопрос соотношения количества независимых каналов шума в системе, и выходная мощность каждого из каналов.

До последнего времени при сравнении систем защиты приоритет отдавался тем системам, к усилителю мощности которых можно под-

ключить как можно больше датчиков. При этом стоимость системы (удельная, приведённая к одному датчику) оказывается минимальной. И что же в результате? К одному каналу приходится подключать, например, вибровозбудители разных типов, которые установлены на абсолютно разных конструкциях (стекло, труба, стена и т. д.). Один канал — одна настройка. Оптимально «настроить» такую систему невозможно в принципе. Настраивать приходится «по слабому звену», а остальные датчики будут создавать повышенный паразитный шум в помещении.

Противоположная крайность, хотя и очень заманчивая, — система «один канал — один датчик», т. е. система с большим числом маломощных каналов. В настоящее время конструктивно это решено применением виброизлучателей, в состав которых входит индивидуальный генератор. Идеально настраиваемая, но довольно дорогая система. Данную систему целесообразно использовать при наличии большого числа ограждающих конструкций разнообразного типа.

Компромисс, как правило, где-то посередине. Оптимальными являются системы многоканальные, позволяющие подключить на один канал не более 3...5 датчиков. При этом выходная мощность одного канала обычно должна быть в диапазоне 2...4 Вт. Именно таким образом построенные системы можно признать оптимальными.

Выходные каскады усилителей (каналов) обычно строятся по типовым схемам и какими-либо особенностями не обладают. Исключение составляют усилители мощности класса «Д», поскольку они работают принципиально в нелинейном режиме. Каким образом именно такой режим работы может повлиять на свойства шумового сигнала, придется еще установить. Однако применение режима «Д» никем не запрещено, поэтому не является недостатком с точки зрения регламентирующих документов.

Последним рассматриваемым элементом являются акустические излучатели и вибровозбудители. Моделей их множество, и в настоящее время они приблизительно равносильны. Одни более пригодны для массивных, другие — для менее массивных конструкций; электромагнитные, электродинамические, пьезоэлектрические — у всех есть плюсы и минусы. Как правило, важны КПД преобразователя и равномерность АЧХ. Хотя невозможно рассматривать эти параметры в отрыве от той поверхности, на которую установлен преобразователь. Поэтому этот вопрос надо решать в каждом конкретном случае в привязке к конкретной задаче. Разумеется, более универсальными выглядят системы, способные работать с датчиками различных типов и принципов действия. Так как в каждом конкретном случае в зависимости от различных факторов выбор может быть разнообразен, оставим его заказчику системы защиты.

4.1.4. Защита системы электропитания

Акустические закладки, транслирующие информацию по линиям электросети, модулируя ею ВЧ несущие и другие информативные сигналы, нейтрализуются помехоподавляющими фильтрами в этих линиях.

Разделительные трансформаторы могут применяться только при достаточно низкочастотных опасных сигналах, обычно это не выше 1 МГц. Нежелательные резистивные и емкостные связи между обмотками устраняют с помощью внутренних экранов и элементов, имеющих высокое сопротивление изоляции. Степень снижения уровня наводок достигает 40 дБ.

Основное назначение помехоподавляющих фильтров — пропускать без ослабления сигналы, частоты которых находятся в пределах рабочего диапазона, и подавлять сигналы, частоты которых находятся вне этих пределов.

Фильтры нижних частот пропускают сигналы с частотами ниже его граничной частоты (частоты среза). Одним из распространённых типов сетевых помехоподавляющих фильтров являются фильтры серии ФСПК. Их типовые параметры давно известны и приводятся в табл. 4.5.

Помехоподавляющие фильтры типа ФСПК устанавливают в осветительную и розеточную сети вблизи трансформаторной подстанции или на выходе силовых кабелей из здания. В некоторых случаях допускается их установка на месте их выхода из выделенных помещений.

Следует отметить, что помехоподавляющие фильтры этого типа малочувствительны к длине шлейфа заземления корпусов фильтров, что выделяет их из ряда аналогичных изделий.

В качестве активных средств для зашумления линий электропитания используют генераторы электромагнитного шума SELSP-44, «Соната-РС1», «Соната-РК1», «Соната», «Гном-ЗИ4» и многие другие.

Таблица 4.5

Характеристика	Тип фильтра			
	ФСПК-10	ФСПК-40	ФСПК-100	ФСПК-200
Номинальный ток, А	10	40	100	200
Номинальное напряжение (фаза–земля) переменного тока 50 Гц, В	220	220	220	220
Вносимое затухание, дБ	Не менее 60			
Число фильтруемых линий	3	2	4 на 2 корпуса	
Масса, кг	5,5	10	16×2	18×2

4.1.5. Защита оконечного оборудования слаботочных линий

За счет микрофонного эффекта или ВЧ навязывания практически все оконечные устройства телефонии, систем пожарно-охранной сигнализации, трансляционного вещания и оповещения, содержащие элементы, подверженные акустоэлектрическим преобразованиям, создают в подводящих линиях электрические сигналы. Уровень создаваемых сигналов может составлять от единиц нановольт до десятков милливольт. Так, например, элементы звонковой цепи телефонного аппарата под действием акустических колебаний амплитудой ≈80 дБ подают в линию преобразованный сигнал напряжением ≈10 мВ. При тех же условиях подобный сигнал электродинамического громкоговорителя имеет уровень до 30 мВ. Трансформированный, он может возрасти до 500 мВ и стать доступным для перехвата на расстоянии до 100 м. Облучающий сигнал навязывания благодаря высокой частоте проникает в гальванически отключенную микрофонную цепь положенной телефонной трубки и модулируется информационным сигналом.

Пассивная защита от микрофонного эффекта и ВЧ навязывания осуществляется ограничением слабых сигналов и фильтрацией или отключением линии, по которой распространяется опасный сигнал.

В схемах ограничителей используют встречно-параллельно включенные полупроводниковые диоды, сопротивление которых для малых (преобразованных) сигналов, составляющее десятки мегаом, препятствует их прохождению в слаботочную линию. Для токов большой амплитуды, соответствующих полезным сигналам, сопротивление оказывается равным сотням Ом и они свободно проходят в линию.

При применении такого рода ограничителей (на встречно-параллельных диодах) необходимо учитывать, что они эффективны только в цепях без протекания постоянного тока. Постоянные токи даже самых малых значений (порядка долей и единиц мкА) «открывают» диоды и при этом сопротивление цепочки резко падает. Следовательно, устройство перестаёт быть эффективным средством защиты.

Фильтрация является достаточо эффективным средством борьбы с ВЧ навязыванием. При этом роль простейших фильтров могут выполнять конденсаторы, включаемые в микрофонную и звонковую цепи. Шунтируя высокочастотные сигналы навязывания, они не оказывают мешающего влияния на полезные сигналы.

Для защиты телефонных аппаратов, как правило, используют приборы, сочетающие свойства фильтра и ограничителя. Вместо устаревшего устройства «Гранит» применяют сертифицированные изделия «Корунд» и «Грань-300». К сожалению, эти устройства неэффективны для современных ТА, потребляющих от линии ток для питания некоторых микросхем в схеме ТА.

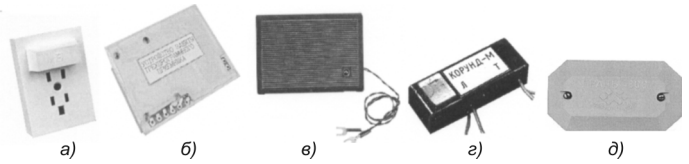


Рис. 4.15. Внешний вид устройств МП-1А (*а*), МП-2 (*б*), МП-4 (*в*), «Корунд» (*г*), «Грань» (*д*)

Активная защита оконечных устройств осуществляется маскированием полезных сигналов. Изделия серии МП, снабженные фильтрами от ВЧ навязывания, генерируют в линии шумоподобные колебания. Устройство МП-1А (для аналоговых линий) реализует этот режим при положенной телефонной трубке в речевом диапазоне, а МП-1Ц (для цифровых линий) — в более широком диапазоне частот. Защиту трехпрограммных трансляционных приемников обеспечивают приборы МП-2 и МП-3, вторичных электрочасов — МП-4, динамиков оповещения — МП-5, который дополнительно гальванически отключает их от линии при отсутствии полезных сигналов.

Следует учитывать, что генераторы шума, встроенные в устройства МП-1, нормально функционируют только при постоянном напряжении в линии не менее 35...37 В. В некоторых моделях современных АТС напряжении в линии поддерживается на значительно более низком уровне, что делает применение этих средств защиты неэффективным.

Внешний вид устройств МП-1А, МП-2, МП-3, МП-4, «Корунд», «Грань» приведен на рис. 4.15.

Так как известные устройства защиты, встраиваемые в ТА цифровых линий, обеспечивают отключение микрофона телефонной трубки и микрофона громкоговорящей связи в режиме ожидания вызова (трубка лежит на телефоне). Однако при этом остаются подключенными такие акустоэлектрические преобразователи, как телефонный капсюль телефонной трубки и динамик громкоговорящей связи, которые могут создавать канал утечки информации. Кроме того, данные устройства не обеспечивают отключение режима прослушивания помещения (часто его неправильно называют «полицейский режим»).

Устройство защиты МП-7 «Гвард» (рис. 4.16) предназначено для защиты ТА цифровых АТС от несанкционированного доступа по абонентской сети — прослушивания через акустоэлектрические преобразователи телефона. Оно обеспечивает защиту ТА цифровых линий от утечки через него акустических

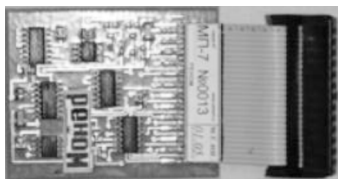


Рис. 4.16. Устройство защиты МП-7 «Гвард»

сигналов помещений через все акустоэлектрические преобразователи ТА и исключает возможность прослушивания помещения при положенной трубке аппарата.

Защита абонентского участка телефонной линии. Телефонная линия может использоваться в качестве источника питания или канала передачи информации акустической закладки, установленной в помещении. Пассивная защита абонентской линии предполагает блокирование акустических закладок, питающихся от линии, при положенной телефонной трубке. Активная защита производится зашумлением абонентской линии и уничтожением акустических закладок или их блоков питания высоковольтными разрядами.

К основным способам защиты абонентской линии относятся:

- подача в линию во время разговора маскирующих низкочастотных сигналов звукового диапазона или ультразвуковых колебаний;
- поднятие напряжения в линии во время разговора или компенсация постоянной составляющей телефонного сигнала постоянным напряжением обратной полярности;
- подача в линию маскирующего низкочастотного сигнала при положенной телефонной трубке;
- генерация в линию с последующей компенсацией на определенном участке абонентской линии сигнала речевого диапазона с известным спектром;
- подача в линию импульсов напряжением до 1500 В для выжигания электронных устройств и блоков их питания.

4.1.6. Защита информации, обрабатываемой техническими средствами

Физические основы возникновения ПЭМИН от информативных сигналов в цепях ТСПИ и ОТСС уже рассмотрены выше, как и каналы утечки по отходящих проводным линиям.

В рамках приведённой модели необходимого (ниже нормированного) отношения сигнал/шум можно добиться, как и при рассмотрении других каналов утечки, уменьшая величину сигнала или увеличивая уровень шума. Как и в других областях, меры и средства защиты подразделяются на пассивные и активные. Дополнительной особенностью защиты ТСПИ и ОТСС является то, что защищаемая информация существует в виде токов или напряжений в их цепях большой амплитуды (величины). Естественно, большой по сравнению с аналогичными сигналами в цепях ВТСС. Как правило, это единицы–десятки вольт или миллиампер. Тем не менее, такие сигналы порождают вполне заметные магнитные и электрические поля и наводки.

Экранирование. Экранирование применяется по отношению как к элементам ТС (соединительные кабели, узлы, блоки и устройства

в целом), как и к их комплексам и/или помещениям в целом. Различают электростатическое, магнитостатическое и электромагнитное экранирования.

Основная задача электростатического экранирования состоит в уменьшении емкостных связей между защищаемыми элементами и сводится к обеспечению накопления статического электричества на экране с последующим отводом зарядов на землю. Применение металлических экранов позволяет полностью устранить влияние электростатического поля.

Эффективность электрического экранирования зависит от частоты и электрических свойств материала экрана. Начиная с частот порядка сотен кГц эффективен экран из любого металла толщиной от 0,5 до 1,5 мм, для частот свыше десятков МГц подобный же результат дает металлическая фольга толщиной около 0,1 мм. Заземление экрана не влияет на эффективность экранирования.

Высокочастотное электромагнитное поле ослабляется полем обратного направления, создаваемым вихревыми токами, наведенными в металлическом сплошном или сетчатом экране. Экран из медной сетки 2×2 мм ослабляет сигнал на 30...35 дБ, двойной экран — на 50...60 дБ. Однако применение двойного сетчатого экрана осложняется резонансными явлениями в зазоре между отдельными экранами, на частотах которых ослабление резко снижается.

Наряду с узлами приборов экранируются монтажные провода и соединительные линии. Длина экранированного монтажного провода не должна превышать четверти длины самой короткой волны в составе спектра сигнала, передаваемого по проводу. Высокую степень защиты обеспечивают витая пара в экранированной оболочке и высокочастотные коаксиальные кабели. Наилучшую защиту от электрического и магнитного полей гарантируют линии типа бифиляра, трифиляра, изолированного коаксиального кабеля в электрическом экране, металлизированного плоского многопроводного кабеля.

Частичное ослабление в распространение электромагнитного поля вносят и неметаллические или композитные конструкции.

В табл. 4.6 приведены данные, характеризующие степень ослабления высокочастотных электромагнитных полей различными зданиями.

В последнее время начали появляться специализированные материалы, предназначенные для экранирования/поглощения электромагнитной энергии. Это многочисленные модели поглощающих элементов типа ферритовых поглощающих насадок (фильтров) для кабелей (как круглых, так и плоских), самые разнообразные фильтрующие элементы для разъёмов, гибкие прокладки на базе тех же материалов, кирпич и штукатурки на базе шунгита и его композиций.

Таблица 4.6

Тип здания	Степень экранирования, дБ, на частоте, МГц		
	100	500	1000
Кирпичное здание с толщиной стен 1,5 кирпича	13...15	15...17	16...19
Железобетонное здание с ячейкой арматуры 15×15 см и толщиной стен 16 см	20...25	18...19	15...17

Заземление. Экранирование эффективно только при правильном заземлении аппаратуры ОТСС и ТСПИ и соединительных линий. Система заземления должна состоять из общего заземления, заземляющего кабеля, шин и проводов, соединяющих заземлитель с экранами. Качество электрических соединений должно обеспечивать минимальное сопротивление контактов, их надежность и механическую прочность в условиях вибраций и жестких климатических условиях. В качестве заземляющих устройств запрещается использовать «нулевые» провода электросетей, металлоконструкции зданий, оболочки подземных кабелей, трубы систем отопления, водоснабжения, сигнализации.

Значение сопротивления току растекания заземляющего устройства определяется удельным сопротивлением грунтов, зависящим от влажности почвы, состава, плотности, температуры. Значения этого параметра для различных грунтов приведены в табл. 4.7.

Орошение почвы вокруг заземлителей 2...3%-ным соляным раствором снижает сопротивление заземления в 5...10 раз.

Сопротивление заземления, Ом, выполненного в виде вертикально вбитой трубы, определяется выражением

$$R_1 = \frac{\rho}{2\pi l}\left(\ln\frac{8}{D_\text{т}} - 1\right),$$

где l — длина трубы, см; $D_\text{т}$— диаметр трубы, см.

Сопротивление заземления ТСПИ и ОТСС не должно превышать, в соответствии с ПУЭ, 4 Ом, и для достижения этого значения применяют многоэлементное заземление из ряда одиночных, симметрично расположенных заземлителей, соединенных между собой шинами при

Таблица 4.7

Тип грунта	Удельное сопротивление ρ, Ом/см^3		
	среднее	минимальное	максимальное
Золы, шлаки, соляные отходы	2370	500	7000
Глина, суглинки, сланцы	4060	340	16300
То же с примесями песка	15800	1020	135000
Гравий, песок, камни с небольшим количеством глины или суглинков	94000	59000	458000

помощи сварки. Магистрали заземления вне здания прокладывают на глубине 1,5 м, а внутри здания таким образом, чтобы их можно было проверять внешним осмотром. Устройства ТСПИ (ОТСС) подключают к магистрали болтовым соединением в одной точке.

Требования нормативных документов, относящиеся к размещению заземляющего устройства, относительно границ контролируемой зоны во многих случаях могут быть выполнены созданием глубинного заземлителя. Эта конструкция представляет собой скважину глубиной до нескольких десятков метров (обычно — углублённую на 5...7 м в близлежайший водонесущий слой) и размещённую вблизи или в цокольном этаже (подвале) здания. Обсадная труба, опущенная в такую скважину, нижняя часть которой находится в водоносном горизонте, обеспечивает крайне низкое сопротивление току растекания. Разумеется, толщина стенки такой трубы должна быть достаточной, чтобы в условиях омывания грунтовыми водами обеспечить срок службы не менее 10...15 лет. Практически идеальна труба из нержавеющей стали (например, ХН9Т, ХН10Т), но это недешёвое решение.

Существующая сегодня техника позволяет выполнять такое бурение в любом помещении цокольного этажа. Разумеется, выбор точки для устройства глубинного заземлителя, кроме требований по защите информации, должен предусматривать внимательное рассмотрение структуры почвы в районе здания и согласование с соответствующими службами возможности размещения глубинного заземлителя в выбранной зоне, чтобы не повредить никакие подземные коммуникации.

4.2. Организация защиты информации от утечки, возникающей при работе вычислительной техники, за счет ПЭМИН

Стабильность поступления сведений, неявная, скрытая от владельца, форма съема информации, обрабатываемой техническими средствами, обусловили неослабевающий интерес к каналу утечки, возникающему за счет побочных электромагнитных излучений и наводок (ПЭМИН), сопровождающих работу этой аппаратуры.

Ниже дается характеристика каналов утечки, описываются методология и способы защиты информации от утечки за счет ПЭМИН. Рассматриваются пути реализации и характеристики современных активных средств защиты — генераторов шума, приводятся рекомендации по их применению.

Характеристика канала утечки информации за счет ПЭМИН. Частотный диапазон побочных электромагнитных излучений, сопровождающих информативные сигналы, простирается от единиц килогерц до гигагерц и выше и определяется крутизной фронтов импульсов

цифровых кодов, циркулирующих в цепях используемого средства обработки информации (ОТСС). Так, для стандартного современного компьютерного монитора перехват информации возможен на частотах вплоть до 1000-й гармоники тактовой частоты, а уровень излучения, составляющий в ближней зоне до десятков дБ, позволяет принимать сигналы на удалении до нескольких сотен метров.

Возникающие электромагнитные излучения вокруг средств обработки информации вызывают наводки на близко расположенные кабели, телефонные провода, линии охранно-пожарной сигнализации, электросеть и т. п. Интенсивность полей в диапазоне частот от единиц килогерц до сотен мегагерц такова, что прием сигналов может вестись за пределами контролируемой зоны (КЗ) при непосредственном подключении к этим линиям.

4.2.1. Методология защиты информации от утечки за счет ПЭМИН

В зависимости от среды распространения информативных сигналов рассматривают два возможных канала утечки: собственно за счет ПЭМИ и наводки на коммуникации.

Канал ПЭМИ характеризуется размером «зоны 2» (R_2) — расстоянием между ОТСС и условной границей, за пределами которой невозможен эффективный прием вследствие естественного снижения уровня излучаемого сигнала. Значение R_2 рассчитывается по результатам специальных исследований и задаётся «в сфере», т. е. в трёх измерениях.

Канал случайных антенн характеризуется размерами их «зоны 1» (r_1, r_1') для сосредоточенных случайных антенн (ССА) и распределенных случайных антенн (РСА). К сосредоточенным случайным антеннам относятся любые технические средства, имеющие выход за пределы контролируемой зоны. К распределенным случайным антеннам относят провода, кабели, элементы конструкций здания и т. п. Расстояние между ОТСС и СА, на котором невозможен эффективный перехват, определяет размер зоны 1 (также «в сфере»).

Проведенный анализ позволяет сделать определенные выводы и сформулировать критерии оценки защищенности ОТСС от утечки через ПЭМИ и наводки. ОТСС считается защищенным, если:

- радиус зоны 2 для любого устройства, входящего в его состав и в любом режиме функционирования, не превышает минимально допустимого расстояния от ОТСС до границы КЗ;
- радиус зоны 1 для любого устройства, входящего в его состав и в любом режиме функционирования, не превышает минимально допустимого расстояния от ОТСС до ССА и РСА либо отношение мощностей информативного сигнала нормированной помехи

во всех СА не превышает на границе КЗ предельно допустимую величину;

- отсутствуют отходящие от ОТСС коммуникации (выходящие за пределы КЗ) либо отношение мощностей информативного сигнала к нормированной помехе в них на границе КЗ не превышает предельно допустимую величину.

Критерии защищенности СВТ. Критерием оценки защищенности средств вычислительной техники (СВТ) является сформулированное ранее условие: если для устройства ОТСС отношение сигнал/шум (Δ) на входе приемного устройства перехвата информации ограниченного пользования не превышает предельно допустимого значения δ во всех возможных каналах утечки, т. е. если

$$\delta \geqslant \Delta = U_{\text{с пик}}/U_{\text{ш эфф}},$$

то устройство защищено от утечки. Объект считается защищенным в целом, если защищено каждое устройство.

Измеренное отношение опасный сигнал/помеха (Δ) — отношение амплитуды импульсного сигнала $U_{\text{с пик}}$ к среднеквадратичному напряжению помехи $U_{\text{шэфф}}$ на входе приемного устройства.

Для объектов категории 1 — это квазиоптимальный приемник импульсных сигналов во всём диапазоне существования опасных сигналов. Для объектов категории 2 и 3 — квазиоптимальный приемник импульсных сигналов с полосой пропускания $\Delta f = 1/\tau$, где τ — длительность импульса.

Нормы на отношение опасного сигнала к шуму (помехе) δ относятся к последовательным и параллельным кодам, а также учитывают многократное повторение информации. Излучение одного разряда — это такое излучение, которое характерно для этого разряда в отсутствии излучений других разрядов машинной ячейки и каких-либо иных излучений. Если измерено суммарное излучение большого числа разрядов (но не более 16), то необходимо произвести расчет энергии на один разряд. Параллельные коды разрядностью более 16 считаются неопасными.

Если измерено суммарное излучение нескольких разрядов (но не более 16), то необходимо произвести нормирование этого излучения на один разряд делением его на экспериментально определяемый коэффициент, эквивалентный условному числу разрядов в коде, либо на $n/2$, где n — число разрядов.

При регулярных повторениях сигнала норма предельно допустимого отношения сигнал/помеха ($\delta_{\text{п}}$) определяется по формуле

$$\delta_{\text{п}} = \delta/\sqrt{K_{\text{п}}},$$

где $K_{\text{п}}$ — число повторений.

Нормированные уровни помех в каналах утечки. Нормированные помехи по напряженности электрического ($E_{\text{ш н}}$) и магнитного ($H_{\text{ш н}}$) полей, мкВ/м, для объектов всех категорий приведены в виде аналитических выражений и графиков в нормативных документах.

Шумы (помехи) в линиях определяют из шумов в эфире, умноженных на значение «антенного фактора» РСА. В принятой терминологии понятие «антенного фактора» совпадает по значению, размерности и физическому смыслу с действующей высотой антенны (случайной антенны). Значение антенного фактора предполагается измерять на требуемых частотах в соответствии с установленной методикой.

Основные задачи и принципы защиты СВТ. Для защиты информационных сигналов СВТ от возможной утечки информации применяются организационные и технические мероприятия.

Организационные мероприятия направлены на то, чтобы, не изменяя уровня ПЭМИН средства ЭВТ или уровня электромагнитных шумов, тем или иным способом изменить либо размещение ТС, либо границы контролируемой зоны с тем, чтобы зона возможного перехвата информации была меньше, чем $R_{\text{кз}}$ (контролируемая зона на объекте), т. е. $R_2 < R_{\text{кз}}$.

К техническим мероприятиям защиты информации в СВТ относятся меры и средства, воздействующие либо на уровень ПЭМИН, либо на уровень электромагнитных шумов. Например, электромагнитное экранирование — эффективный способ защиты информации, однако требует значительных экономических затрат и регулярного контроля эффективности экранирования. Кроме того, полное электромагнитное экранирование вносит дискомфорт в работу обслуживающего персонала.

Доработка СВТ позволяет существенно уменьшить уровень информационных излучений, однако полностью устранить их нельзя. В современных условиях доработка техники СВТ сводится к подбору комплектующих СВТ, так как собственные разработки средств ЭВТ в РФ отсутствуют и сборка ПЭВМ происходит из зарубежных комплектующих. При подборе комплектующих на сборочных фирмах (красная сборка) обращается внимание на материнскую плату, конструктивное выполнение корпуса системного блока, видеокарту (видеоконтроллер), тип дисплея и т. д. Кроме того, применяются меры локального экранирования, установка заграждающих и поглощающих фильтров и другие меры.

Активная радиомаскировка, зашумление — применение широкополосных генераторов шума. Основная задача зашумления эфира — поднять уровень электромагнитного шума и тем самым препятствовать радиоперехвату информационных сигналов СВТ. Показателем

эффективности заградительной шумовой помехи (шум с нормальным законом распределения мгновенных значений амплитуд) является отношение сигнал/шум. Техническое средство СВТ будет защищено, если это отношение меньше нормированного.

4.2.2. Некоторые особенности контроля ТКУИ для СВТ

Наиболее массовым объектом возникновения каналов утечки информации и, в силу этого, объектом инструментального контроля (специальных исследований) являются объекты СВТ.

Однако сегодняшняя ПЭВМ, и автономная, и являющаяся элементом распределённой сети, состоит из большого числа отдельных устройств, функционирующих по своим алгоритмам, со своими протоколами обмена, цифровыми кодами, тактовыми частотами и т. д. Правильная системная оценка, грамотный инженерный анализ, предшествующий самим специальным исследованиям, во многом обеспечивает как надёжность результатов, так и минимизацию затрат на осуществление защиты в целом.

Основные исходные положения. Из материалов, приведённых выше для ТКУИ за счёт ПЭМИН, можно сделать вывод, что при рассмотрении утечки информации в форме существования в виде цифрового кода наиболее «опасны» коды последовательные, одноразрядные. Причём это утверждение остаётся справедливым на протяжении уже не одного десятка лет.

Рассмотрим типовой состав ПЭВМ (рабочего места, АРМ) под этим углом зрения и выявим узлы, блоки, устройства, использующие последовательные коды. Прежде всего, определим, что считать типовым составом.

Следует особо отметить, что применение на ПЭВМ, ведущей обработку закрытой информации (т. е. на ОТСС), устройств, использующих какие-либо беспроводные интерфейсы подключения (радиоканал, ИК канал), кроме волоконно-оптических (ВОЛС), категорически запрещено. В связи с этим «радиоклавиатуры», мыши, ТВ тюнеры и прочую современную удобную периферию мы не рассматриваем принципиально! Протоколы IR Wave, 802.11 (с любыми индексами), BlueTooth, Wi-Fi, WiMAX и т. д. запрещены в принципе.

Примем за типовой следующий состав:

1. Системный блок в комплектации:

- «материнская» плата;
- накопитель на жёстком магнитном диске (HDD);
- звуковая карта;
- видеокарта;
- накопитель на оптическом диске (CD, DVD, CD-R, DVD-R или «комбидрайв»);

- сетевая карта (на медной паре или оптическая);
- порты.
  2. Клавиатура.
  3. Манипулятор «Мышь».
  4. Монитор.
  5. Принтер.
  6. Сканер (планшетный или объединённый с принтером).

Рассмотрение более «экзотических» устройств оставим за пределами данного издания.

Рассмотрим представленный перечень основных устройств ПЭВМ несколько подробнее под профессиональным углом зрения. На материнской плате практически весь обмен между смонтированными на ней устройствами осуществляется по 32-разрядной шине (процессор, память, «северный» и «южный» мосты, слоты для вставных карт, IDE- и SATA-контроллеры и т. д.). Следовательно, в наше поле зрения всё это не попадает.

«Жёсткие диски» в настоящее время существуют двух основных типов: с интерфейсом IDE или SATA. Первый из них параллельный и в связи с его высокой разрядностью рассмотрению не подлежит, второй — последовательный. Также отдельно необходимо рассматривать узел записи (головку и её цепи), которые, однозначно, относятся к устройствам последовательного кодирования.

Звуковая карта, как правило, весьма редко используется для обработки защищаемой информации. Это случается только в вариантах применения ПЭВМ в системах обработки аудиоинформации. Тогда звуковая карта рассматривается и как ОТСС, и как ТСПИ со всеми вытекающими последствиями. Тем не менее, отметим что, как правило, цифровой аудиосигнал обрабатывается этим устройством в 16-разрядном коде (в наиболее «продвинутых — до 24 разрядов) или в аналоговой форме.

Современные видеокарты в зависимости от подключаемого монитора и ряда иных факторов получают сигнал от системной шины в виде 32-разрядного кода. Затем направляют его в монитор либо в аналоговой форме по интерфейсу RGB, либо в форме цифровой, по интерфейсу DVI. При этом аналоговый интерфейс RGB, несмотря на свою «трёхразрядность» (три физических аналоговых линии, красная, зелёная, синяя), приравнивается к последовательной кодировке. А DVI именно таковым и является изначально (особенно при видеоразрешении до 1600×1280). На более высоких разрешениях включаются два параллельных канала передачи данных.

Устройства чтения или чтения/записи на оптических дисках (CD, DVD) на сегодняшний день подключаются к контроллеру на материнской плате по интерфейсу либо IDE (параллельному), либо SATA (пос-

ледовательному). При чтении дисков интерфейс является определяющим, а вот в режимах записи лазерный диод и его цепи — пример устройства с последовательным кодированием.

Клавиатура, точнее её интерфейс (на сегодняшний день порты PS/2 или USB), являются классическими последовательными интерфейсами.

Манипулятор «мышь», подключаемый либо по COM-порту (устарел и не применяется), либо по USB, также последовательный, но информация о положении курсора мыши на экране не несёт никакой реальной информации и защите не подлежит.

Мониторы в настоящее время представлены на рынке двумя основными типами — CRT и TFT. Первые, на основе электронно-лучевой трубки, как устройства отображения сдают свои позиции. Их заменяют «плоские» и значительно более лёгкие и экономичные модели с ЖКИ экраном. Однако с точки зрения образования возможных каналов утечки сегодняшние TFT-модели гораздо более опасны. Дело в том, что схемотехника их построения предусматривает не только интерфейс связи с системным блоком (видеокартой), но и несколько внутренних интерфейсов обработки данных (RSDS, LVDS и их модификации). Несмотря на то что эти интерфейсы имеют разрядность от 18 до 24, ряд особенностей вынуждает применять к ним принципы и подходы для последовательного кода. ПЭМИН этих узлов TFT монитора имеет значительные величины и весьма информативен.

С принтерами вопрос тоже не слишком прост. Их моделей много, как и принципов действия. Кроме того, как чаще всего и бывает, интерфейс подключения это одно, а собственно принтер, его узлы обработки данных и печать — совсем другое. На сегодняшний день для подключения принтеров применяются порты LPT (устаревший и редко применяемый) и USB. Первый 8-разрядный параллельный, второй последовательный.

Подавляющее большинство существующих принтеров в настоящее время являются либо лазерными, либо струйными. Необходимо отметить, что в лазерных принтерах узлы лазерного диода рассматриваются как устройство с последовательным кодированием. А в струйных принтерах печатающая головка и цепи её управления являются устройством с параллельным кодированием. Число «разрядов» очень различается от модели к модели и требует специального определения. Однако уровень ПЭМИН из этого узла зачастую столь значителен, что результаты расчётов даже с учётом коэффициента разрядности порядка 20 дают значения зоны 2 до десятков метров.

Так же следует рассматривать и печатающие узлы ныне почти исчезнувших матричных принтеров с числом «иголок» от 8 до 12.

При рассмотрении сканеров, в подавляющем числе случаев, основное внимание необходимо сосредоточить именно на интерфейсе подключения. На сегодняшний день для подключения сканеров применяются порты LPT (устаревший и редко применяемый), SCSI (как правило, 16-разрядный) и USB.

В заключение рассмотрим порты общего применения, размещаемые на системном блоке. Порты COM, LPT и USB были рассмотрены выше. Далее следует порт IEEE1394 (Firewire, i.LINK) и порты сетевой карты. Fi-Wi — классический последовательный порт, как и сетевой порт (выход/вход сетевой карты).

Таким образом, выявляется набор устройств, узлов и интерфейсов, которые должны быть рассмотрены в первую очередь как наиболее опасные с точки зрения потенциальной возможности образования канала утечки за счёт ПЭМИН.

4.2.3. Некоторые особенности ПЭМИН и контроля защищённости устройств и интерфейсов ПЭВМ

Опустим рассмотрение интерфейсов LPT, COM и 16-разрядного SCSI как малоактуальных в настоящее время. Применение порта IEEE 1394 сейчас нарастает, но он применяется, как правило, при обработке (передаче) видеоинформации. Этот случай не столь часто встречается в практике и поэтому в данном издании не рассматривается.

Накопитель на жёстком магнитном диске («хард-диск», HDD). IDE интерфейс контролю не подлежит в связи с его многоразрядностью. SATA (SATA2) надо контролировать, но результаты этого контроля весьма разные. На настоящее время с этим интерфесом ещё не всё отработано. Ожидаемые частоты появления ПЭМИН примерно кратны 400 МГц. Однако уровень ПЭМИН крайне нестабилен и зависит от множества факторов. Регистрируется, как правило, по электрической компоненте поля на расстояниях не более 1 м. Если корпус системного блока вносит заметное ослабление, то ПЭМИ не выявляется при применении средств измерения среднего класса (по собственным шумам).

ПЭМИН пишущей головки и её цепей носит совсем иной характер и выявляется, как правило, по магнитной компоненте поля на расстояниях 0,3...0,5 м. Тактовые частоты $F_т$ ориентировочно (например, для диска фирмы Western Digital с пятью пластинами емкостью 4 Тбайт) составляют

$$F_т = N_c n K_c K_б \approx 128000 \cdot 7200 \cdot 4096 \cdot 8 = 6{,}6 \cdot 10^{12} \approx 6{,}6 \text{ ГГц},$$

где N_c — число секторов на одном треке, равное 128000; n — число оборотов диска в с, равное 7200; K_c — число байт в секторе (длина сектора), 4096; $K_б$ — число битов в байте, 8.

Число секторов на треке и длина сектора выявляется с помощью ряда прикладных программ работы с HDD на физическом уровне типа Acronis True Image или Partition Magic. Число оборотов шпинделя в минуту — в паспортных данных HDD. Спектр ПЭМИН, как правило, имеет характер не «линейчатый», а зон со сплошным спектром вокруг ожидаемых частот. Это связано с фазовой модуляцией тока записи в головке, обусловленной современными методами записи. В ряде случаев ПЭМИН узлов записи может фиксироваться на расстоянии до 1...1,5 м от системного блока.

Накопитель на оптическом диске (CD-R, DVD-R). Почти во всём с точки зрения образования ПЭМИН является аналогом жёсткого диска. Как по интерфейсу, так и по узлам записи. Скорость записи и иные параметры устанавливаются исходя из режима «кратности» скорости записи, с учетом того, что «однократная скорость» соответствует 600 кбайт/с. Бóльшая часть параметров устанавливается в программе записи, например Nero, работа в которой (запись на болванку) и применяется в качестве тест-режима. Заранее сформированный файл с подготовленной информацией размером 700 или 4700 Мб записывается на диск, что занимает вполне достаточное для проведения СИ время.

Сетевая карта. Вопросы специальных исследований сетевых карт на сегодняшний день, как ни странно, недостаточно проработаны. Протоколы обмена, принятые для LAN, меняются так быстро, что разработки способов и режимов выявления и измерения ПЭМИН отстают. Однозначно это разработано только для давно устаревшего и, практически неприменяемого, протокола обмена со скоростью 10 Мбит/с. Для наиболее распространённого протокола (по витой паре) 100 Мбит/с разработка режима СИ затруднена построением самого протокола. Дело в том, что аппаратная его часть, с целью повышения достоверности, кодирует каждый следующий байт иной последовательностью импульсов в самой витой паре. В результате невозможно создать тест-режим, при котором чередование «нулей» и «единиц» происходит с постоянной тактовой частотой. Как следствие — невозможность выявления и измерения фиксированных частот и применения установленного метода расчёта. Есть некоторые косвенные приёмы, основанные на измерениях и расчёте сплошных спектров, возникающих в данном случае, но их подробное рассмотрение выходит за рамки данного издания. Тем не менее, в большом числе практических случаев выявление, измерение и оценка уровней сплошного псевдошумового сигнала от кабелей локальной сети (и сетевых карт) возможно.

Порты USB. Специальные исследования портов USB в настоящее время являются непременной составляющей СИ вообще. Как прави-

Рис. 4.17. Кадры данных интерфейса USB

ло, этот порт задействован, практически, всегда – для подключения принтера, сканера, «флеш-памяти» и т. д. Учитывая разнообразие качества кабелей, их разнообразную длину и очень высокую скорость обмена, следует знать, что ПЭМИН именного этого порта может дать в результате значительные значения R_2.

В спецификации USB 2.0 радикально повышена пропускная способность шины. Первоначально (в версиях 1.0 и 1.1) шина обеспечивала две скорости передачи информации: низкую скорость (Low Speed, LS) 1,5 Мбит/с и полную скорость (Full Speed, FS) 12 Мбит/с. В версии 2.0 определена еще и высокая скорость (High Speed, HS) 480 Мбит/с, что позволяет существенно расширить круг устройств, подключаемых к шине. В одной и той же системе могут присутствовать и одновременно работать устройства со всеми тремя скоростями. Допустимая длина сегмента (кабеля от устройства до хаба) — до 5 м. Ограничения на длину сегмента диктуется затуханием сигнала и вносимыми задержками. Шина позволяет с использованием промежуточных хабов соединять устройства, удаленные от компьютера на расстояние до 30 м (5 хабов, 6 кабельных сегментов).

Хост организует обмены с устройствами согласно своему плану распределения ресурсов. Для этого хост-контроллер циклически с периодом 1 мс формирует кадры (frames), в которые укладываются все запланированные транзакции. Каждый кадр (рис. 4.17) начинается с посылки пакета-маркера SOF (Start Of Frame), который является синхронизирующим сигналом для изохронных устройств, а также для хабов. Кадры нумеруются последовательно, в маркере SOF передаются 11 младших битов номера кадра. В режиме HS каждый кадр делится на 8 микрокадров, и пакеты SOF передаются в начале каждого микрокадра (с периодом 125 мкс). При этом во всех восьми микрокадрах SOF несет один и тот же номер кадра. Новое значение номера кадра передается в нулевом микрокадре. В каждом кадре (микрокадре) может быть выполнено несколько транзакций, их допустимое число зависит от скорости, длины поля данных каждой из них, а также от задержек, вносимых кабелями, хабами и устройствами. Все транзакции кадров должны быть завершены до начала интервала времени EOF (End of Frame). Период (частота) генерации кадров (микрокадров) может немного варьироваться с помощью специального регистра хост-контроллера, что позволяет подстраивать частоту для изохронных передач.

Кадрирование используется и для обеспечения живучести шины. В конце каждого кадра (микрокадра) выделяется интервал времени EOF, на время которого хабы запрещают передачу по направлению к контроллеру. Если хаб обнаружит, что с какого-то порта в это время ведется передача данных (к хосту), этот порт отключается, изолируя «болтливое» устройство, о чем информируется USBD. Хост планирует загрузку кадров так, чтобы помимо запланированных изохронных транзакций и прерываний в них всегда находилось место для транзакции управления. Свободное время кадров может заполняться передачами массивов.

Рекомендуется использовать для тестирования порта (кабеля) специально подготовленное устройство флэш-памяти, так как это самый простой вариант (обычно устройство флэш-памяти с элементами экранирования, чтобы снизить ПЭМИН самой флэшки). Естественно, устройство должно поддерживать версию протокола, соответствующую версии, поддерживаемой подключаемым к порту реальным устройством (принтером, сканером и т. д.).

При организации тестового режима в программе «Сигурд-Тест» используется вкладка записи на диск таким образом, что в записываемом на флэш-диск байте все разряды будут нести логическую единицу, т. е. импульс (максимальный энергетический режим). Для протоколов USB 1.0 и USB 1.1 получим спектр по форме, аналогичный спектру ЭЛТ-монитора с тактовыми частотами соответственно 1,5 и 12 МГц.

Информативный сигнал USB порта легко верифицируется, огибающая сигнала в режиме верификация надёжно распознаётся системой «Сигурд».

Что же касается протокола USB 2.0, то устройства, осуществляющие обмен информацией под его управлением самостоятельно, в зависимости от условий передачи сообщений устанавливают скорость передачи данных, начиная с максимальной HS 480 Мбит/с. При сбоях в канале, осуществляется переход на FS 12 Мбит/с, далее на скорость LS 1,5 Мбит/с. Причем хост-контролер может осуществлять кодирование одного и того же байта различными кодовыми посылками. При этом может возникнуть спектр сигнала, показанный на рис. 4.18.

Спектр сигнала расширяется с увеличением центральной частоты. При этом псевдотактовая частота («несущая») не является информативной. Информативным является сигнал «подставки» видимого сплошного спектра. Выполнение операции поиска и верификации таких информативных сигналов ПЭМИ приходится производить вручную.

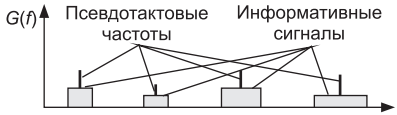


Рис. 4.18. Ожидаемый спектр информативного сигнала интерфейса (порта) USB 2.0

Клавиатура. Внутренний контроллер клавиатуры способен определить факты нажатия и отпускания клавиш, при этом можно нажимать очередную клавишу, даже удерживая несколько ранее нажатых. При нажатии клавиши клавиатура передает идентифицирующей ее скан-код. При удержании клавиши в нажатом положении через некоторое время клавиатура начинает автоповтор передачи скан-кода нажатия этой клавиши. Задержка автоповтора (typematic delay) и скорость автоповтора (typematic rate) для клавиатур AT программируются. Автоповтор с точки зрения центрального процессора работает следующим образом. Если нажать клавишу, контроллер выработает прерывания и выдаст скан-код нажатия. Если клавишу удерживать нажатой, то через некоторое время задержки (typematic delay) клавиатура начнет генерировать серию посылок скан-кода, и они будут вызывать серию прерываний IRQ1 с передачей этого кода до тех пор, пока не будет отпущена клавиша.

При нажатии клавиши «= » («+ ») скан-код представляет из себя меандр с тактовой частотой работы внутреннего контроллера, как правило, это 6...10 кГц ± 10...15%. Именно таким образом задается тестовый сигнал для проверки клавиатуры.

Символ, изображенный на нажатой клавише, дублируется в окне Клавиша =, а его код — в окне Код клавиши 187 (рис. 4.19, код клавиши «187» соответствует символу «= »). Естественно верифицировать данный сигнал можно только вручную.

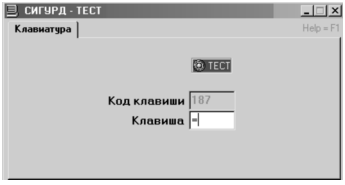


Рис. 4.19. Вид рабочего окна программы «Сигурд-Тест» в режиме проверки клавиатуры

Для клавиатур характерна нестабильность тактовой частоты задающего генератора, поэтому она подвержена паразитной высокочастотной генерации. Следовой уровень излучения от клавиатуры может наблюдаться до частот 10...15 МГц, выше крайне редко.

Ожидаемый спектр информативного сигнала от клавиатуры на экране системы «Сигурд» показан на рис. 4.20.

Как видно из рисунка, спектр от клавиатуры линейчатый, сосредоточен в основном на частотах от 10 до 400 кГц с шагом 6...10 кГц. Поиск и измерение ОС сильно затруднены неинформативным ПЭМИН импульсных блоков питания системного блока (в диапазоне от единиц кГц до первого десятка МГц).

Кроме того, для клавиатуры достаточно часто характерны явления паразитных высокочастотных возбуждений (ПВЧГ) на частотах сотен кГц — десятков МГц.

Монитор. Специальные исследования CRT мониторов и их RGB интерфейса в данном издании не рассматриваются в связи с полной

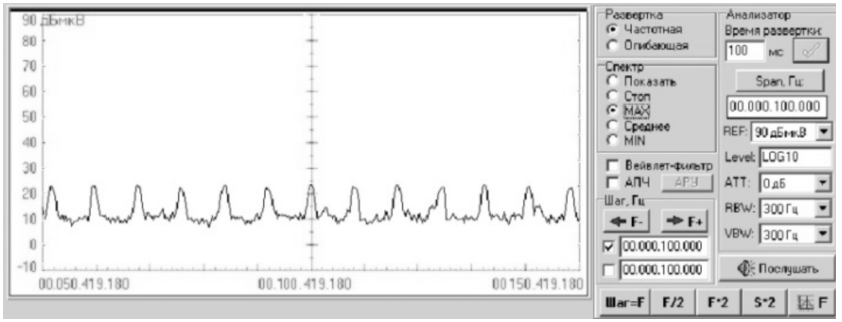


Рис. 4.20. Ожидаемый спектр информативного сигнала от клавиатуры

разработанностью данного вопроса и отсутствием каких-либо «подводных камней». Рассмотрим вопросы, связанные с исследованием ПЭМИН внутренних интерфейсов мониторов, которые упоминались ранее.

В ЖК дисплеях управление осуществляется всеми ячейками одной строки одновременно, а не последовательно, как пробегает луч ЭЛТ. Это позволяет увеличить время, в течение которого производится управление ячейкой.

В любом случае аналоговые сигналы RGB от VGA-интерфейса непосредственно использоваться для управления матрицей не могут. В ЖК дисплеях эти сигналы оцифровываются, полученные значения (для каждого пикселя) сохраняются в буферной памяти и оттуда уже построчно выводятся на матрицу. Все эти действия возложены на интерфейсы внутренней дисплейной шины, такие как LVDS, mini LVDS или RSDS.

Так как сигналы выводятся на каждый субпиксель строки параллельно, а количество пикселей в строке достаточно большое, то сигналы управления самими ЖК ячейками не создают информативных ПЭМИ и измерять их не надо.

Еще раз вспомним, каким образом образуются цветовые оттенки в ЖК мониторах. За счет поворота на определенный угол ЖК молекул в каждом из цветовых субпикселов (ЖК ячейке), можно получать не только открытое и закрытое её состояния, но и промежуточные, формирующие цветовой оттенок. Теоретически угол поворота ЖК молекул можно сделать любым в пределах от минимального до максимального. Кроме того, для формирования произвольного уровня напряжения потребуется использование схем ЦАП с большой разрядностью, что крайне дорого. При использовании 18 битов на пиксель на каждый цветовой канал приходится по 6 битов. Это позволяет сформировать 64 ($2^6 = 64$) различных уровня напряжения и соответственно задать 64 различные ориентации ЖК молекул, что, в свою

очередь, приводит к формированию 64 уровней яркости в одном цветовом канале. Всего же, смешивая цветовые уровни разных каналов, можно получить 262144 цветовых оттенка. При использовании 24 битов на пиксель, на каждый канал приходится по 8 битов, что позволяет сформировать уже 256 ($2^8 = 256$) уровней яркости в каждом канале, а всего такая матрица воспроизводит 16 777 216 цветовых оттенков.

Таким образом, у сигналов на входе микросхем управления столбцами ЖК матрицы (Column Driver) код с разрядностью 6 или 8 передается последовательно, пиксель за пикселем, с кроссшины в память драйверов столбцов с заданной тактовой частотой. Эти сигналы и вызывают появление информативных ПЭМИ. Причем при снятии информации по каналу ПЭМИН потенциальному противнику, по большому счету, все равно какого цвета будет буква. При перехвате информации ему достаточно решить бинарную задачу — светлый или тёмный пиксель. Для восстановления алфавитно-цифрового и большей части графических изображений более, чем достаточно. То есть передача по внутренней шине 18- или 24-разрядного кода эквивалентна передаче одноразрядного последовательного кода.

Поэтому для проверки ЖК монитора можно применить точно такой же тест «пиксель через пиксель», обеспечивающий максимальную энергетику информативного сигнала, как и для ЭЛТ-монитора. Казалось бы, при такой организации внутреннего интерфейса ЖК монитора спектр информативного сигнала должен быть достаточно простым и соответствовать по форме спектру ЭЛТ-монитора. Однако этого не происходит. Все дело в том, что сигналы внутреннего интерфейса имеют высокую тактовую частоту, а фронты импульсов очень малой длительности. Физические двухпроводные линии на кросс-плате достаточно протяжённы (20...40 см), и их симметрирование не идеально. При этом создаются такие излучения, которые не вписываются в нормы по допустимому уровню электромагнитных излучений.

Если бы тактовые частоты внутреннего интерфейса монитора были постоянны, то и спектр ПЭМИ этих составляющих был бы линейчатым и они фиксировались бы на вполне определённых частотах. Значения их (по напряжённости поля) были бы весьма высоки. Производители ЖК матриц и схем их управления вынуждены «укладываться» в довольно жёсткие международные нормы по ПЭМИ с точки зрения электромагнитной совместимости и вреда для здоровья людей. Приборы (индикаторы), которыми измеряют напряжённости поля ПЭМИ для контроля стандартов ISO, DIN и др., имеют фиксированную полосу пропускания 120 кГц. В целях «заметания мусора под ковер» внутренние интерфейсы ЖК мониторов меняют тактовую частоту обработки информации по закону, показанному на рис. 4.21.

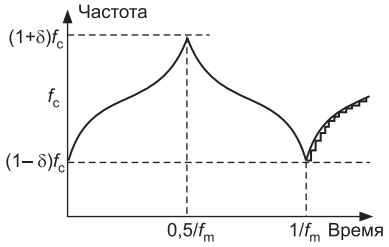


Рис. 4.21. Закон модуляции тактовой частоты

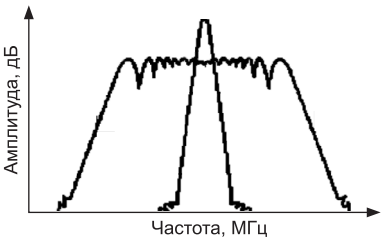


Рис. 4.22. Вид спектра сигнала при модуляции тактовой частоты

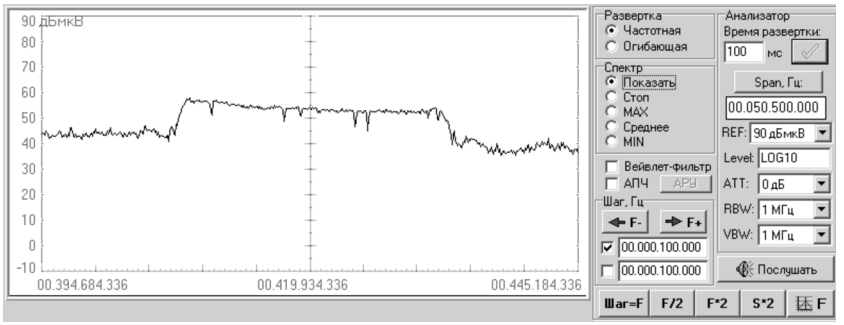


Рис. 4.23. Вид спектра сигнала при разрешении по частоте 1 МГц

В результате этого энергетика ПЭМИ как бы размазывается по широкому спектру и в измеряемых полосах пропускания приемника его уровень становится удовлетворяющим норме (рис. 4.22).

Вид спектра сигнала при разрешении 1 МГц показан на рис. 4.23. В центре — полоса пропускания стандартного измерителя.

При изменении тактовой частоты по закону Hersey kiss (дословно «поцелуй Херши»), показанному на рис. 4.21, получается сплошной спектр (рис. 4.23), неоднородный по краям, что хорошо видно при полосе пропускания приемника 10 кГц (рис. 4.24).

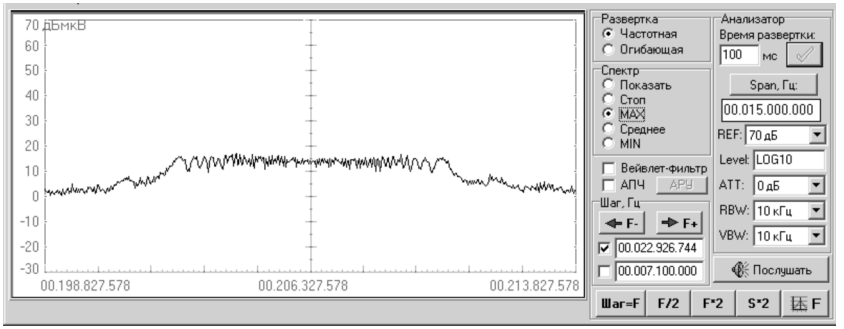


Рис. 4.24. Вид спектра сигнала при разрешении по частоте 10 кГц

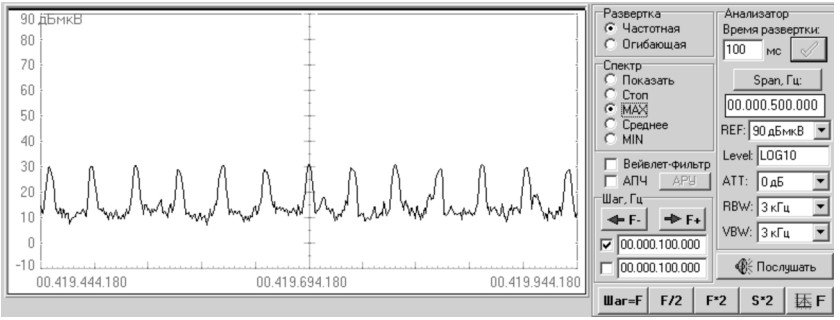


Рис. 4.25. Вид спектра при разрешении по частоте 3 кГц

Если бы меняющий тактовую частоту сигнал изменялся плавно, то получился бы истинно сплошной спектр, но он изменяется дискретно, поэтому и получаются сотни спектральных составляющих с малым шагом по частоте. Сигнал как бы расплывается, распадаясь на множество составляющих. Вид спектра сигнала с разрешением 3 кГц показан на рис. 4.25.

При выполнении проверки ЖК-мониторов операции поиска и верификации информативных сигналов ПЭМИ внутренних интерфейсов приходится производить вручную. Ни один автоматизированный комплекс облегчить работу оператора при этих действиях пока не способен в силу широкополосности этих сигналов ПЭМИН (полоса, занимаемая сигналом, доходит до 30...50 МГц).

Кроме этого, всё больше специалистам приходится встречаться с внешним интерфейсом DVI, т. е. цифровым интерфейсом подключения монитора (рис. 4.26). У этого интерфейса существует ряд особенностей, которые необходимо учитывать.

В протоколе TMDS, на котором основан DVI, на каждый цветовой канал отводится по восемь битов, что позволяет получить 256 уровней яркости каждого базового цвета. Если перемножить 256 уровней у трёх цветов, то мы получим 16,7 миллиона оттенков.

Графический чип создаёт информацию о цвете для каждого пикселя в 24-битном потоке (8 битов на цвет). Поток параллельных данных поступает на передатчик протокола TMDS, который преобразует его в три последовательных потока, передающихся по трём физическим симметричным парам одновременно. Когда сигнал поступает на приёмник (в мониторе), то его последовательный код вновь преобразуется в параллельный. Преобразование в последовательный сигнал для передачи по кабелю необходимо, поскольку последовательная передача менее подвержена помехам, чем параллельная, особенно на больших расстояниях. Таким образом, данный цифровой поток, являясь трёхразрядным, в силу полной синхронности фронтов

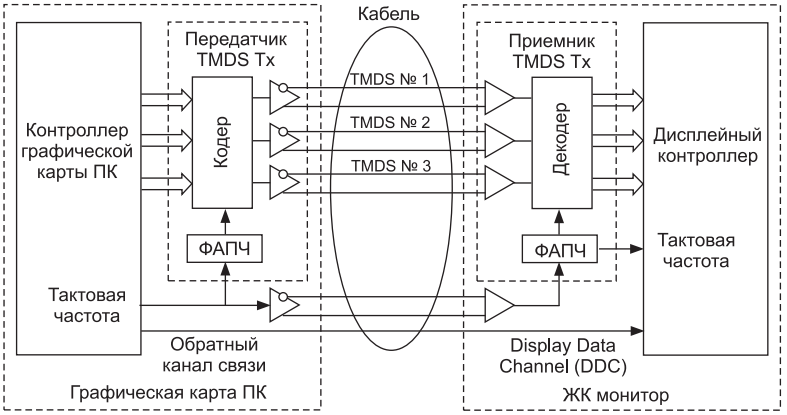


Рис. 4.26. Блок-схема DVI интерфейса

в каждом цветовом канале (формируется в одном кристалле, от одного тактового генератора) рассматривается как последовательный одноразрядный.

TMDS-передатчик (Transition Minimized Differential Signaling) отсылает последовательный сигнал по четырём разным каналам кабеля: один для тактового сигнала, а три — для цветовой информации. Восемь битов информации для каждого цвета передаются в последовательном 10-битном сигнале: восемь битов для цветовых данных, а также два служебных. Данные передаются в 10 раз быстрее тактового генератора из-за использования ФАПЧ-чипа, работающего как умножитель частоты. Таким образом, скорость 1,65 Гбайт/с достигается при номинальной частоте 165 МГц.

Протокол TMDS построен на минимизации числа переходов от 0 к 1 (и наоборот), что позволяет надёжнее передавать информацию по медному кабелю. Минимизация числа переходов делает тракт менее чувствительным к внешним помехам и снижает уровень ПЭМИН (рис. 4.27).

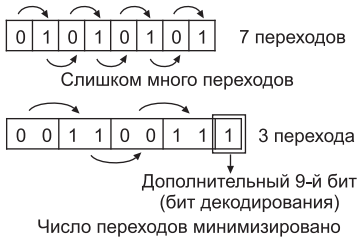


Рис. 4.27. Принцип перекодирования протокола TDMS

Такое построение (кодирование) информации в линии передачи (в кабеле к монитору) усложняет задачу создания тест-режима с постоянной тактовой частотой переходов от 0 к 1 в кабеле. Для теста, априори, исходя из структуры интерфейса, необходимо либо кодировать цвет в каждом пикселе последовательностью 10101010, либо применять иные методы. В противном случае нельзя будет применять установленный метод расчёта результатов.

Рис. 4.28. Кодирование в TDMS длинных неизменных последовательностей

При использовании типовой программы «Сигурд-Тест» возможен один такой вариант, не требующий изменения этой тест-программы. Учитывая, что в стандартном тесте чередуются белые и чёрные пиксели, а белый пиксель это код 255;255;255 (FF;FF;FF), то в цифровом потоке передаётся три байта единиц без переходов тока. Такой случай у TDMS-интерфейса рассматривается особо.

Если к проводу долгое время подводится ток (относительно долго, поскольку скорости передачи очень высоки), то перед его спадом должно пройти определённое время. В таких случаях могут возникнуть проблемы передачи, к примеру, если длительное время будут передаваться одни единицы (состояние «1» = есть ток), а затем поток данных прервётся одним нулём (состояние «0» = нет тока). В зависимости от качества медного кабеля этот нуль можно потерять. В результате один из пикселей будет отображён неверно. Бит DC-Balanced указывает на обычную инверсию значений восьми битов, чтобы предотвратить длительную передачу одинаковых данных по кабелю (рис. 4.28).

Таким образом, мы получаем для такой информации (сплошные единицы) передачу пакетов нулей и единиц с одним переходом от 0 к 1 или наоборот на границе пакета (т. е. инверсию каждого второго пакета). Следовательно, получается постоянная тактовая частота сигнала в кабеле интерфейса, близкая к значению 130...165 МГц (т. е. к максимальной частоте передачи пикселей — пакетов). Следует отметить, что за счёт некоторых особенностей протокола частоты режима «пиксель через пиксель» и просто «белый экран» отличаются приблизительно на 4...6 %, оставаясь постоянными.

Расчёт результатов СИ от DVI интерфейса при таком тест-режиме уже не вызывает никаких трудностей (подробное рассмотрение расчёта и значений всех параметров расчётного соотношения выходит за рамки данного издания). Уровень ПЭМИН от образца к образцу

довольно сильно разнится, что связано, по всей видимости, с качеством и симметрией пар в интерфейсном кабеле.

Разрешение монитора во время проведения СИ рекомендуется устанавливать не выше 1600×1280 (при 60 Гц кадровой частоты), чтобы не включался второй канал интерфейса. Процедура СИ в режиме параллельной работы двух каналов дополнительно усложняет интерпретацию результатов СИ.

Принтер. Возможные внешние интерфейсы принтеров (любых) уже рассмотрены выше, поэтому сосредоточимся на рассмотрении СИ печатающих узлов.

Для лазерного принтера это сам лазерный диод и цепи его управления. Кодирование информации, т. е. импульсов тока, вызывающих засветку на вращающемся фотобарабане, естественно, последовательное. Тест-режим типовой, типа «пиксель через n пикселей», практически как для RGB-интерфейса монитора. Длительность импульса и его тактовую частоту для выбранного режима проще всего измерить прямо на диоде (обычно порядка первых единиц МГц). Априорный расчёт этих значений затруднён неизвестной скоростью вращения фотобарабана, вращающейся призмы (зеркала) и другими неизвестными факторами. Сами СИ трудностей не представляют, уровень сигналов, как правило, низкий, ПЭМИН регистрируются не далее 0,3. . . 0,5 м от лазерного диода.

Струйные принтеры построены на различных принципах формирования микрокапель чернил.

В электростатических принтерах из сопла выбрасывается непрерывная серия капель — технология называется CIJ (Continuous Ink Jet). С помощью управляющего электрода часть капель отклоняется в сборник (на рециркуляцию), часть летит на бумагу. Есть вариант технологии и с «каплями по требованию» (Drop On Demand, DOD), без рециркуляции; эта печать происходит медленнее.

В пьезоэлектрических принтерах (основная технология фирмы Epson) капли выстреливаются механическими микронасосами на пьезоэлементах. Управляемость размером капли и отсутствие «сателлитов» (мелких брызг вокруг основной капли) — свойства, полезные при полутоновой печати.

В пузырьковых принтерах (bubble-jet), выпускаемых фирмами HP, Lexmark, Canon, Xerox, капля выталкивается пузырьком пара (от микроскопического нагревательного элемента). Взрыв плохо управляем, вокруг капли присутствуют мелкие «сателлиты». Ресурс головок ограничен, но они дешевые и легко меняются. Разрешение — до 1200–2400 dpi.

Число сопел в головке измеряется десятками и сотнями, одновременно могут срабатывать несколько сопел. Очевидно, что информа-

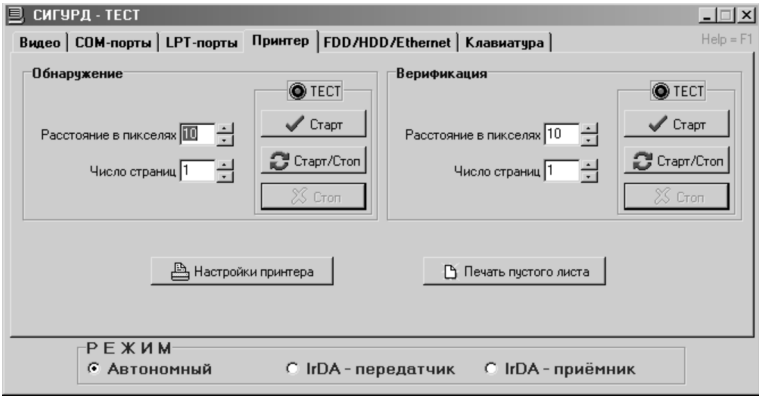


Рис. 4.29. Вид рабочего окна программы «Сигурд-Тест» в режиме проверки принтера

тивные ПЭМИ с максимальными уровнями будут создавать сигналы управляющие соплами, которые проходят по плоскому кабелю подвода к фильерам, он и будет являться излучающей антенной. Естественно, тактовая частота следования управляющих импульсов будет зависеть от скорости печати и составлять десятки килогерц. В электростатических и пьезоэлектрических принтерах управление соплами производится напряжением, и от них следует ожидать преобладающей электрической составляющей поля. В пузырьковых принтерах управление производится током и преобладающей составляющей поля ПЭМИ будет магнитная.

Наиболее энергетическим также будет являться тест пиксел через пиксель, но часто удобнее применять режим «пиксель через 5–10 пикселей». Вид рабочего окна программы «Сигурд-Тест» в режиме проверки принтера показан на рис. 4.29.

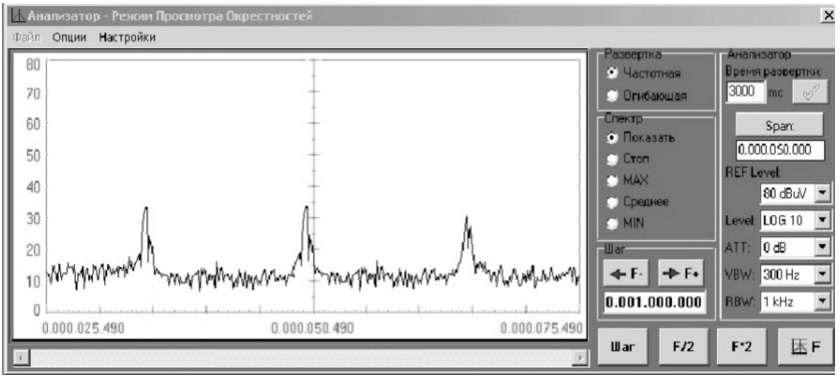


Рис. 4.30. Ожидаемый спектр информативного сигнала от струйного принтера

Ожидаемый спектр информативного сигнала от струйного принтера показан на рис. 4.30. Уровни ПЭМИН, как правило, весьма значительные (по отношению к другим источникам). Поиск и измерение опасных сигналов затруднены неинформативным ПЭМИН импульсных блоков питания как системного блока, так и самого принтера (в диапазоне от десятков кГц до первого десятка МГц).

4.3. Организация защиты ПЭВМ от несанкционированного доступа

В настоящее время в связи с бурным развитием средств вычислительной техники и появлением новых информационных технологий появилось новое направление добывания категорированной информации, тесно связанное с компьютерной преступностью и несанкционированным доступом (НСД) к информации ограниченного пользования. Развитие локальных и глобальных компьютерных сетей привело к необходимости закрытия несанкционированного доступа к информации, хранящейся в автоматизированных системах.

Целью защиты информации является предотвращение ущерба, возникновение которого возможно в результате утери (хищения, утраты, искажения, подделки) информации в любом ее проявлении.

Любое современное предприятие не может сегодня успешно функционировать без создания надежной системы защиты своей информации, включающей не только организационно-нормативные меры, но и технические программно-аппаратные средства, организации контроля безопасности информации при ее обработке, хранении и передаче в автоматизированных системах (АС).

Организуя защиту информации от несанкционированного доступа, при ее обработке и хранении в автоматизированных системах необходимо учитывать следующие принципы и правила обеспечения безопасности информации.

1. Соответствие уровня безопасности информации законодательным положениям и нормативным требованиям по охране сведений, подлежащих защите по действующему законодательству, в том числе выбор класса защищенности АС в соответствии с особенностями обработки информации (технология обработки, конкретные условия эксплуатации АС) и уровнем ее конфиденциальности.

2. Выявление конфиденциальной (защищаемой) информации и ее документальное оформление в виде перечня сведений, подлежащих защите, его своевременная корректировка.

3. Наиболее важные решения по защите информации должны приниматься руководством предприятия или владельцем АС.

4. Определение порядка установления уровня полномочий пользователей, а также круга лиц, которым это право предоставлено (администраторы информационной безопасности).

5. Установление и оформление правил разграничения доступа (ПРД), т. е. совокупности правил, регламентирующих права доступа субъектов доступа к объектам доступа.

6. Установление личной ответственности пользователей за поддержание уровня защищенности АС при обработке сведений, подлежащих защите.

7. Обеспечение физической охраны объекта, на котором расположена защищаемая АС (территория, здания, помещения, хранилища информационных носителей), с помощью установления соответствующих постов, технических средств охраны или любыми другими способами, предотвращающими или существенно затрудняющими хищение средств вычислительной техники (СВТ), информационных носителей, а также НСД к СВТ и линиям связи.

8. Организация службы безопасности информации (ответственные лица, администратор ИБ), осуществляющей учет, хранение и выдачу информационных носителей, паролей, ключей, ведение служебной информации СЗИ НСД (генерацию паролей, ключей, сопровождение правил разграничения доступа), приемку включаемых в АС новых программных средств, а также контроль за ходом технологического процесса обработки конфиденциальной информации и т. д.

9. Планомерный и оперативный контроль уровня безопасности защищаемой информации, согласно применяемых руководящих документов по безопасности информации, в том числе проверка защитных функций средств защиты информации.

Средства защиты информации должны иметь *сертификат,* удостоверяющий их соответствие требованиям по безопасности информации.

Анализ опыта работ, связанных с обработкой и хранением информации с использованием средств вычислительной техники, позволил сделать выводы и обобщить перечень возможных угроз информации. Условно их можно разделить на три вида:

- нарушение конфиденциальности информации;
- нарушение целостности информации;
- нарушение доступности информации.

Исходя из этого и строится система защиты автоматизированных систем и ПЭВМ от несанкционированного доступа.

Построение системы защиты на базе программно-аппаратного комплекса средств защиты информации от НСД и ее взаимодействие с программно-аппаратным обеспечением ПЭВМ в общем виде приведены на рис. 4.31.

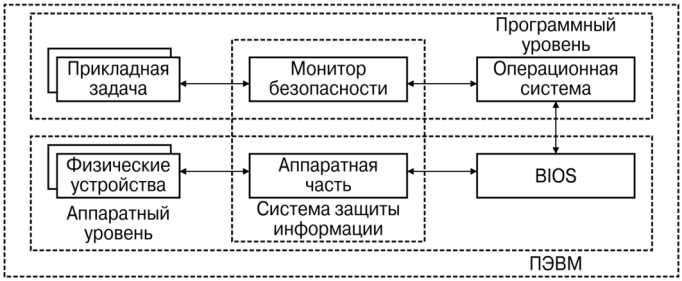


Рис. 4.31. Построение системы защиты на базе программно-аппаратного комплекса

Защита информации с использованием аппаратных и программных средств комплекса защиты от НСД основана на обработке событий, возникающих при обращении прикладных программ или системного программного обеспечения (ПО) к ресурсам ПЭВМ. При этом средства комплекса перехватывают соответствующие программные и/или аппаратные прерывания (запросы на выполнение операций к аппаратным и/или программным ресурсам ПЭВМ). В случае возникновения контролируемого события (запрос прерывания) производится анализ запроса, и в зависимости от соответствия полномочий субъекта доступа (его прикладной задачи), установленных администратором безопасности ПРД, либо разрешают, либо запрещают обработку этих прерываний.

В общем случае система защиты состоит из собственно средств защиты от несанкционированной загрузки ОС и средств разграничения доступа к информационным ресурсам, которые условно можно представить в виде четырех взаимодействующих подсистем защиты информации (рис. 4.32).

Подсистема управления доступом предназначена для защиты ПЭВМ от посторонних пользователей, управления доступом к объектам доступа и организации совместного их использования зарегистрированными пользователями в соответствии с установленными правилами разграничения доступа. Под посторонними пользователями понимаются все лица, не зарегистрированные в системе (не имеющие зарегистрированного в конкретной ПЭВМ персонального идентификатора).

Рис. 4.32. Подсистемы защиты информации

Защита от посторонних пользователей обеспечивается процедурами идентификации (сравнение предъявленного идентификатора с перечнем зарегистрированных на ПЭВМ) и аутентификации (подтверждение подлинности), которая обычно осуществляется при вводе пароля определенной длины. Для идентификации пользователей в комплексах защиты от НСД наиболее часто используются персональные идентификаторы типа TouchMemory (Ibutton) DS 199X, отличающиеся высокой надежностью, уникальностью, наличием быстродействующей памяти, удобством пользования, приемлемыми массогабаритными характеристиками и низкой ценой.

В комплексах защиты от НСД могут быть реализованы два принципа управления доступом к защищаемым ресурсам: дискреционный и мандатный.

Дискреционный принцип управления доступом. Каждому зарегистрированному пользователю устанавливаются права доступа, по принципу присвоения заданных характеристик доступа каждой паре «субъект–объект», которые прописываются в ПРД. При запросе пользователя на доступ обеспечивается однозначное трактование установленных ПРД и в зависимости от уровня полномочий пользователя разрешается или запрещается запрошенный тип доступа.

Данный вариант управления доступом позволяет для любого пользователя системы создать изолированную программную среду, т. е. ограничить его возможности по запуску программ, указав в качестве разрешенных к запуску только те программы, которые действительно необходимы для выполнения пользователем своих служебных обязанностей. Таким образом, программы, не входящие в этот список, пользователь запустить не сможет.

Мандатный принцип управления доступом. Принцип управления доступом к ресурсам ПЭВМ (аппаратным и программным), основанный на сопоставлении уровня конфиденциальности, присваиваемого каждому ресурсу, и полномочиях конкретного зарегистрированного пользователя по доступу к ресурсам ПЭВМ с заданным уровнем конфиденциальности.

При организации мандатного управления доступом для каждого пользователя системы устанавливается некоторый уровень допуска к конфиденциальной информации, а каждому ресурсу (каталоги, файлы, аппаратные средства) присваивается так называемая метка конфиденциальности.

При этом доступ к конфиденциальным каталогам и файлам разграничивается сравнением уровня допуска пользователя и метки конфиденциальности ресурса и принятии решения о предоставлении или не предоставлении доступа к ресурсу.

Подсистема регистрации и учета предназначена для регистрации в системном журнале, представляющем собой специальный файл, размещаемый на жестком диске ПЭВМ, различных событий, происходящих при работе ПЭВМ. При регистрации событий в системном журнале регистрируются:

- дата и время события;
- имя и идентификатор пользователя, осуществляющего регистрируемое действие;
- действия пользователя (сведения о входе/выходе пользователя в/из системы, запусках программ, событиях НСД, изменении полномочий и др.). Доступ к системному журналу возможен только администратору ИБ (супервизору). События, регистрируемые в системном журнале, определяются администратором СЗИ.

Эта подсистема также реализует механизм обнуления освобождаемых областей памяти.

Подсистема обеспечения целостности предназначена для исключения несанкционированных модификаций (как случайных, так и злоумышленных) программной и аппаратной среды ПЭВМ, в том числе программных средств комплекса и обрабатываемой информации, обеспечивая при этом защиту ПЭВМ от внедрения программных закладок и вирусов. В программно-аппаратных комплексах систем защиты информации (ПАКСЗИ) от НСД это обычно реализуется:

- проверкой уникальных идентификаторов аппаратных частей ПЭВМ;
- проверкой целостности назначенных для контроля системных файлов, в том числе файлов в программно-аппаратных комплексах систем защиты информации от НСД, пользовательских программ и данных;
- контролем обращения к операционной системе напрямую, в обход прерываний DOS;
- исключением возможности использования ПЭВМ без аппаратного контроллера комплекса;
- механизмом создания замкнутой программной среды, запрещающей запуск привнесенных программ, исключающих несанкционированный выход в ОС.

При проверке целостности программной среды ПЭВМ вычисляется контрольная сумма файлов и сравнивается с эталонным (контрольным) значением, хранящимся в специальной области данных. Эти данные заносятся при регистрации пользователя и могут изменяться в процессе эксплуатации ПЭВМ. В комплексах защиты от НСД используется сложный алгоритм расчета контрольных сумм — вычисление значения их хэш-функций, исключающий факт необнаружения модификации файла.

Подсистема криптографической защиты предназначена для усиления защиты пользовательской информации, хранящейся на жестком диске ПЭВМ или сменных носителях. Подсистема криптографической защиты информации позволяет пользователю зашифровать или расшифровать свои данные с помощью индивидуальных ключей, как правило, хранящихся в персональном ТМ-идентификаторе.

В состав типового **комплекса защиты ПЭВМ от НСД** входят аппаратные и программные средства. К аппаратным средствам относятся аппаратный контроллер, съемник информации и персональные идентификаторы пользователей.

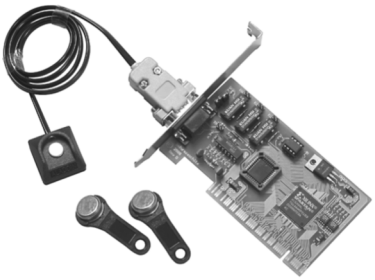


Рис. 4.33. Аппаратный контроллер «Соболь»

Аппаратный контроллер представляет собой плату (ISA/PCI), устанавливаемую в один из слотов материнской платы ПЭВМ (рис. 4.33). Аппаратный контроллер содержит ПЗУ с программным обеспечением, разъем для подключения считывателя информации и дополнительные устройства.

В качестве дополнительных устройств на аппаратном контроллере могут быть установлены реле блокировки загрузки внешних устройств (FDD, CD-ROM, SCSI, ZIP и т. п.), аппаратный датчик случайных чисел и энергонезависимая память.

Считыватель информации представляет собой устройство, предназначенное для считывания информации с предъявляемого пользователем персонального идентификатора. Наиболее часто в комплексах защиты от НСД применяются считыватели информации с персональных идентификаторов типа Touch Memory (Ibutton) DS199X, представляющие собой контактные устройства.

В качестве считывателей информации могут использоваться считыватели смарт-карт (SmartCard Reader) контактные и бесконтактные, а также биометрические считыватели информации, позволяющие идентифицировать пользователя по его биометрическим характеристикам (отпечаток пальца, личная подпись и т. п.).

Персональный идентификатор пользователя представляет собой аппаратное устройство, обладающее уникальными некопируемыми характеристиками. Наиболее часто в системах защиты от НСД используются идентификаторы типа Touch-Memory (Ibutton), представляющие собой электронную схему, снабженную элементом питания и обладающую уникальным идентификационным номером длиной 64 бита, который формируется технологически. Срок эксплуатации электрон-

ного идентификатора, декларируемый фирмой-производителем, около 10 лет.

Помимо ТМ-идентификаторов, в системах защиты от НСД используются идентификаторы типа Smart Card (смарт-карта). Смарт-карта представляет собой пластиковую карточку (рис. 4.34) со встроенной в нее микросхемой, содержащей энергонезависимую перезаписываемую память.

Рис. 4.34. Смарт-карта

Некоторые системы защиты от НСД допускают использование в качестве идентификатора биометрические признаки пользователя (личная подпись, отпечаток пальца и т. п.). Состав программных средств типовой системы защиты информации (СЗИ) от НСД приведен на рис. 4.35.

Все программное обеспечение комплекса защиты от НСД может быть условно разделено на три группы.

Системные программы защиты — программы, выполняющие функции по защите и разграничению доступа к информации. Также с использованием данной группы программ выполняется настройка и управление системой защиты в процессе работы.

Рис. 4.35. Состав программных средств типовой системы защиты информации

Спецзагрузчик — программа, обеспечивающая доверенную загрузку базовой ОС.

Драйвер защиты (монитор безопасности) — резидентная программа, осуществляющая контроль полномочий и разграничение доступа к информационным и аппаратным ресурсам в процессе работы пользователя на АС (ПЭВМ).

Программы установки — доступный только администратору СЗИ набор программ для управления работой системы защиты информации. Данный набор программ позволяет осуществлять штатный процесс установки и удаления системы защиты информации.

Программы системы идентификации/аутентификации представляют собой набор программ для формирования и анализа индивидуальных признаков пользователя, используемых при проведении идентификации/аутентификации. В состав данной группы также входят программы создания и управления базой данных пользователей системы.

Программа обучения — в общем случае представляет собой программу для накопления и анализа индивидуальных признаков пользователя (буквенно-цифровая комбинация персонального пароля, личная подпись, отпечатки пальцев) и выработки индивидуальной характеристики, которая записывается в базу данных.

База пользователей содержит уникальные номера идентификаторов пользователей, зарегистрированных в системе, а также служебную информацию (права пользователей, временные ограничения, метки конфиденциальности и т. д.).

Программа идентификации управляет процессом проведения идентификации пользователя: выдает запрос предъявления идентификатора, производит считывание информации из персонального идентификатора, производит поиск пользователя в базе данных пользователей. В случае, если пользователь зарегистрирован в системе, формирует запрос к базе данных индивидуальных характеристик пользователей.

База данных индивидуальных характеристик содержит индивидуальные характеристики всех пользователей, зарегистрированных в системе, и производит выборку необходимой характеристики по запросу программы идентификации.

Технологические программы представляют собой вспомогательные средства для обеспечения безопасного функционирования системы защиты, доступные только администратору системы защиты.

Программы восстановления станции предназначены для восстановления работоспособности станции в случае аппаратных или программных сбоев. Данная группа программ позволяет восстанавливать

первоначальную рабочую среду пользователя (существовавшую до установки системы защиты), а также восстанавливать работоспособность аппаратной и программной части системы защиты.

Важной особенностью программ восстановления станции является возможность снять систему защиты нештатным образом, т. е. без использования программы установки, вследствие чего хранение и учет данной группы программ должен производиться особо тщательно.

Программа ведения системного журнала предназначена для регистрации в системном журнале (специальном файле) всех событий, возникающих в системе защиты в момент работы пользователя. Программа позволяет формировать выборки из системного журнала по различным критериям (все события НСД, все события входа пользователя в систему и т. п.) для дальнейшего анализа.

Динамика работы комплекса защиты от НСД. Для реализации функций комплекса защиты от НСД применяются следующие механизмы:

- механизм защиты от несанкционированной загрузки ОС, включающий идентификацию пользователя по уникальному идентификатору и аутентификацию подлинности владельца предъявленного идентификатора;
- механизм блокировки экрана и клавиатуры в тех случаях, когда могут быть реализованы те или иные угрозы информационной безопасности;
- механизм контроля целостности критичных, с точки зрения информационной безопасности, программ и данных (механизм защиты от несанкционированных модификаций);
- механизм создания функционально замкнутых информационных систем за счет создания изолированной программной среды;
- механизм разграничения доступа к ресурсам АС, определяемый атрибутами доступа, которые устанавливаются администратором системы в соответствии каждой паре «субъект доступа–объект доступа» при регистрации пользователей;
- механизм регистрации управляющих событий и событий НСД, возникающих при работе пользователей;
- дополнительные механизмы защиты.

На этапе установки комплекса защиты от НСД производятся установка аппаратного контроллера в свободный слот материнской платы ПЭВМ и инсталляция программного обеспечения на жесткий диск.

Настройка комплекса заключается в установлении прав разграничения доступа и регистрации пользователей. При регистрации пользователя администратором системы защиты определяются его права доступа: списки исполняемых программ и модулей, разрешенных к запуску данному пользователю.

На этапе установки также формируются списки файлов, целостность которых проверяется при запуске ПЭВМ данным пользователем. Вычисленные значения хэш-функций (контрольных сумм) этих файлов сохраняются в специальных областях памяти (в некоторых системах заносятся в память персонального ТМ-идентификатора).

Механизм защиты от несанкционированной загрузки ОС реализуется с помощью проведения процедур идентификации, аутентификации и контроля целостности защищаемых файлов до загрузки операционной системы. Это обеспечивается при помощи ПЗУ, установленного на плате аппаратного контроллера, которое получает управление во время так называемой процедуры ROM-SCAN. Суть данной процедуры в следующем: в процессе начального старта после проверки основного оборудования BIOS компьютера начинает поиск внешних ПЗУ в диапазоне от C800:0000 до E000:0000 с шагом в 2K. Признаком наличия ПЗУ является наличие слова AA55H в первом слове проверяемого интервала. Если данный признак обнаружен, то в следующем байте содержится длина ПЗУ в страницах по 512 байт. Затем вычисляется контрольная сумма всего ПЗУ, и если она корректна — будет произведен вызов процедуры, расположенной в ПЗУ со смещением. Такая процедура обычно используется при инициализации аппаратных устройств.

В большинстве комплексов защиты от НСД эта процедура предназначена для реализации процесса идентификации и аутентификации пользователя. При ошибке (отказ в доступе) возврат из процедуры не происходит, т. е. дальнейшая загрузка ПЭВМ выполняться не будет.

При установленном аппаратном контроллере и инсталлированном программном обеспечении системы защиты от НСД, загрузка ПЭВМ осуществляется в следующем порядке:

1. BIOS компьютера выполняет стандартную процедуру POST (проверку основного оборудования компьютера) и по ее завершении переходит к процедуре ROM-SCAN, во время которой управление перехватывает аппаратный контроллер системы защиты от НСД.

2. Осуществляется процесс идентификации пользователя, для чего на монитор ПЭВМ выводится приглашение предъявить свой персональный идентификатор (в некоторых системах защиты одновременно с выводом приглашения запускается обратный отсчет времени, позволяющий лимитировать по времени попытку идентификации).

3. В случае предъявления пользователем идентификатора происходит считывание информации. Если идентификатор не предъявлен, доступ в систему блокируется.

4. Если предъявленный идентификатор не зарегистрирован в системе, то выводится сообщение об отказе в доступе и происходит возврат к п. 2.

5. Если предъявленный идентификатор зарегистрирован в системе, система переходит в режим аутентификации. В большинстве систем защиты от НСД для аутентификации используется ввод персонального пароля.

6. При неправильно введенном пароле происходит возврат к п. 2.

7. При правильно введенном пароле аппаратный контроллер передает управление ПЭВМ и производится штатный процесс загрузки ОС.

Добавим, что многие системы позволяют ограничить количество «неверных» входов, проводя перезагрузку в случае заданного числа отказов.

Устойчивость процедуры идентификации/аутентификации сильно зависит от используемых персональных идентификаторов и алгоритмов подтверждения подлинности пользователя. В случае, если в качестве идентификатора используется ТМ-идентификатор, а процедура аутентификации представляет собой ввод персонального пароля, устойчивость ее к взлому будет зависеть от длины пароля.

При осуществлении контрольных процедур (идентификации и аутентификации пользователя, проверке целостности), драйвер системы защиты от НСД блокирует клавиатуру и загрузку ОС. При касании считывателя информации осуществляется поиск предъявленного ТМ-идентификатора в списке зарегистрированных на ПЭВМ идентификаторов. Обычно список хранится на диске С. Если предъявленный ТМ-идентификатор обнаружен в списке, то в некоторых системах защиты от НСД производится контроль целостности файлов в соответствии со списком, составленным для данного пользователя.

В этом случае при проверке перечня файлов пользователя на целостность вычисляется хэш-функция контрольной суммы этих файлов и сравнивается с эталонным (контрольным) значением, считываемым из предъявленного персонального ТМ-идентификатора. Для проведения процедуры аутентификации предусмотрен режим ввода пароля в скрытом виде — в виде специальных символов (например, символа «*»). Этим предотвращается возможность раскрытия индивидуального пароля и использования утраченного (похищенного) ТМ-идентификатора.

При положительном результате указанных выше контрольных процедур загружается ОС. Если предъявленный пользователем идентификатор не зарегистрирован в списке или нарушена целостность защищаемых файлов, загрузка ОС не производится. Для продолжения работы потребуется вмешательство администратора.

Таким образом, контрольные процедуры: идентификация, аутентификация и проверка целостности, осуществляются до загрузки ОС.

В любом другом случае, т. е. при отсутствии у данного пользователя прав на работу с данной ПЭВМ, загрузка ОС не выполняется.

При выполнении файлов конфигурации CONFIG.SYS и AUTOEXEC.BAT производится *блокировка клавиатуры* и загрузка монитора безопасности системы защиты от НСД, осуществляющего контроль за использованием пользователем только разрешенных ему ресурсов.

Механизм контроля целостности реализуется процедурой сравнения двух векторов для одного массива данных: эталонного (контрольного), выработанного заранее на этапе регистрации пользователей, и текущего, т. е. выработанного непосредственно перед проверкой.

Эталонный (контрольный) вектор вырабатывается на основе хэш-функций (контрольной суммы) защищаемых файлов и хранится в специальном файле или идентификаторе. В случае санкционированной модификации защищенных файлов осуществляется процедура перезаписи нового значения хэш-функций (контрольной суммы) модифицированных файлов.

Механизм создания изолированной программной среды реализуется с использованием резидентной части монитора безопасности системы защиты от НСД. В процессе функционирования системы защиты от НСД резидентная часть монитора безопасности проверяет все загруженные из файла CONFIG.SYS драйверов и обеспечивает оперативный контроль целостности исполняемых файлов перед передачей им управления. Тем самым обеспечивается защита от программных вирусов и закладок. В случае положительного исхода проверки управление передается ОС для загрузки файла на исполнение. При отрицательном исходе проверки запуск программы не происходит.

Механизм разграничения доступа реализуется с использованием резидентной части монитора безопасности системы защиты от НСД, который перехватывает на себя обработку функций ОС (в основном, это прерывание int 21, а также int 25/26, и int 13). Смысл работы данного резидентного модуля в том, что при получении от пользовательской программы запроса, например, на удаление файла, вначале производится проверка наличия таких полномочий у пользователя. Если такие полномочия есть, управление передается обычному обработчику ОС для исполнения операции. Если таких полномочий нет, имитируется выход с ошибкой.

Правила разграничения доступа устанавливаются присвоением объектам доступа атрибутов доступа. Установленный атрибут означает, что определяемая атрибутом операция может выполняться над данным объектом.

Установленные атрибуты определяют важнейшую часть ПРД пользователя. От правильности выбора и установки атрибутов во многом зависит эффективность работы системы защиты. В этой связи

администратор системы защиты должен ясно представлять, от чего и как зависит выбор атрибутов, назначаемых объектам, к которым имеет доступ пользователь. Как минимум, необходимо изучить принцип разграничения доступа с помощью атрибутов, а также особенности работы программных средств, которые будут применяться пользователем при работе.

Программное обеспечение систем защиты от НСД позволяет для каждой пары субъект–объект определить (часть указанных характеристик доступа или все):

для дисков:

- доступность и видимость логического диска;
- создание и удаление подкаталогов;
- переименование файлов и подкаталогов;
- открытие файлов для чтения и записи;
- создание и удаление файлов;
- видимость файлов;
- исполнение задач;
- наследование подкаталогами атрибутов корневого каталога (с распространением прав наследования только на следующий уровень либо на все следующие уровни);

для каталогов:

- доступность (переход к данному каталогу);
- видимость;
- наследование подкаталогами атрибутов каталога (с распространением прав наследования только на следующий уровень либо на все следующие уровни);

для содержимого каталога:

- создание и удаление подкаталогов;
- переименование файлов и подкаталогов;
- открытие файлов для чтения и записи;
- создание и удаление файлов;
- видимость файлов;

для задач:

- исполнение.

Механизм регистрации управляющих событий и событий НСД содержит средства выборочного ознакомления с регистрационной информацией, а также позволяет регистрировать все попытки доступа и действия выделенных пользователей при их работе на ПЭВМ с установленной системой защиты от НСД. В большинстве систем защиты от НСД администратор имеет возможность выбирать уровень детальности регистрируемых событий для каждого пользователя.

Регистрация осуществляется в следующем порядке:

1) для каждого пользователя администратор системы устанавливает уровень детализации журнала;

2) для любого уровня детализации в журнале отражаются параметры регистрации пользователя, доступ к устройствам, запуск задач, попытки нарушения ПРД, изменения ПРД;

3) для среднего уровня детализации в журнале отражаются дополнительно все попытки доступа к защищаемым дискам, каталогам и отдельным файлам, а также попытки изменения некоторых системных параметров;

4) для высокого уровня детализации в журнале отражаются дополнительно все попытки доступа к содержимому защищаемых каталогов;

5) для выделенных пользователей в журнале отражаются все изменения ПРД.

Кроме этого, предусмотрен механизм принудительной регистрации доступа к некоторым объектам.

В общем случае системный журнал содержит следующую информацию:

- дата и точное время регистрации события;
- субъект доступа;
- тип операции;
- объект доступа. Объектом доступа может быть файл, каталог, диск. Если событием является изменение прав доступа, то отображаются обновленные ПРД;
- результат события;
- текущая задача — программа, функционирующая на станции в момент регистрации события.

Дополнительные механизмы защиты от несанкционированного доступа к ПЭВМ позволяют повысить уровень защиты информационных ресурсов, относительно базового уровня, достигаемого при использовании штатных функций системы защиты. Для повышения уровня защиты информационных ресурсов целесообразно использовать следующие механизмы защиты:

- ограничение времени «жизни» пароля и его минимальной длины, исключая возможность быстрого его подбора в случае утери пользователем персонального идентификатора;
- использование временны́х ограничений для входа пользователей в систему установки для каждого пользователя интервала времени по дням недели, в котором разрешена работа;
- установка параметров управления хранителя экрана — гашение экрана через заранее определенный интервал времени (в случае если в течение указанного интервала действия оператором не

выполнялись). Возможность продолжения работы предоставляется только после проведения повторной идентификации по предъявлению персонального идентификатора пользователя (или пароля);

- установка для каждого пользователя ограничений по выводу защищаемой информации на отчуждаемые носители (внешние магнитные носители, порты принтеров и коммуникационных устройств и т. п.);
- периодическое осуществление проверки целостности системных файлов, в том числе файлов программной части системы защиты, а также пользовательских программ и данных;
- контроль обращения к операционной системе напрямую,в обход прерываний ОС, для исключения возможности функционирования программ отладки и разработки, а также программ «вирусов»;
- исключение возможности использования ПЭВМ при отсутствии аппаратного контроллера системы защиты для исключения возможности загрузки операционной системы пользователями со снятой системой защиты;
- использование механизмов создания изолированной программной среды, запрещающей запуск исполняемых файлов с внешних носителей либо внедренных в ОС, а также исключающей несанкционированный вход незарегистрированных пользователей в ОС;
- индикация попыток несанкционированного доступа к ПЭВМ и защищаемым ресурсам в реальном времени с помощью подачи звуковых, визуальных или иных сигналов.

Контрольные вопросы для самостоятельной работы

1. Назовите организационные меры, которые нужно принять для защиты объекта.
2. Какую цель преследуют поисковые мероприятия?
3. Назовите пассивные и активные методы технической защиты.
4. Перечислите методы защиты речевой информации.
5. Какая разница между звукоизоляцией и виброакустической защитой помещения?
6. Каким образом нейтрализуются звукозаписывающие устройства и радиомикрофоны?
7. Дайте характеристики устройств защиты оконечного оборудования слаботочных линий.
8. Перечислите способы защиты абонентских телефонных линий.
9. Какова основная цель экранирования?
10. Перечислите требования, предъявляемые к устройствам заземления.
11. Сравните защитные свойства сетевых помехоподавляющих фильтров и генераторов зашумления сети питания. Укажите области применения данных изделий.
12. Назовите технические мероприятия защиты информации в СВТ.
13. Перечислите основные критерии защищенности СВТ.

14. Порядок и особенности проведения специальных исследований технических средств ЭВТ.

15. В чем сущность графического метода расчета радиуса зоны II (R_2)?

16. Основное назначение комплексов защиты от несанкционированного доступа.

17. Что такое персональный идентификатор? Какие виды идентификаторов применяются в системах защиты от НСД? Назовите основные свойства идентификатора.

18. Какие процедуры выполняются системой защиты от НСД до момента загрузки ОС?

19. Что выполняется в процессе аутентификации? Какие виды процессов аутентификации применяются в системах защиты от НСД?

20. Чем определяется стойкость процесса идентификации/аутентификации?

21. Что понимается под определением права разграничения доступа?

22. Что понимается под объектом доступа?

23. Как реализуется мандатный принцип разграничения доступа?

24. Какие подсистемы входят в состав средств разграничения доступа?

25. Какие аппаратные ресурсы входят в типовой состав системы защиты от НСД?

26. Какие параметры регистрируются в системном журнале в процессе работы пользователя? Для чего ведется системный журнал?

27. Какие системы защиты от НСД могут применяться в АС, обрабатывающих информацию, составляющую государственную тайну?

5 МЕРОПРИЯТИЯ ПО ВЫЯВЛЕНИЮ КАНАЛОВ УТЕЧКИ ИНФОРМАЦИИ

Методы и порядок проведения работ по выявлению технических каналов утечки информации, как правило, регламентированы нормативно-методическими документами, в которых определен необходимый вид проведения исследований и работ.

В данных документах определен перечень видов исследований, охватывающий весь спектр работ по выявлению технических каналов утечки информации:

- специальные проверки (СП);
- специальные обследования (СО);
- специальные исследования (СИ), включающие в себя:

а) специальные исследования побочных электромагнитных излучений и наводок;

б) специальные исследования линий электропередач;

в) специальные исследования акустических и вибрационных каналов.

При защите информации, отнесенной к государственной тайне, перечень и виды необходимых исследований и проверок изложен в нормативно-методических документах, и руководителям соответствующих организаций и предприятий требуется только их неуклонно выполнять.

Несколько по другому обстоят дела в коммерческих структурах при защите конфиденциальности коммерческой и другой информации, отнесенной к информации ограниченного доступа. К такой информации в соответствии с требованиями ФЗ №152 «О персональных данных» и раскрывающего его требования постановления Правительства РФ от 17 ноября 2007 г. № 781 относятся и персональные данные. В Положении «Об обеспечении безопасности персональных данных при их обработке в информационных системах» определены требования по организации защиты персональных данных. В частности, в нем говорится: «Для обеспечения безопасности персональных данных при их обработке в информационных системах осуществляется защита речевой информации и информации, обрабатываемой техническими средствами, а также информации, представленной в виде ин-

формативных электрических сигналов, физических полей, носителей на бумажной, магнитной, магнитно-оптической и иной основе».

Таким образом, в настоящее время практически любое предприятие независимо от формы собственности обязано осуществлять защиту персональных данных от утечки по техническим каналам, а следовательно, специалисты, осуществляющие защиту, должны четко представлять, как выявить тот или иной канал утечки и определить необходимые и достаточные меры для защиты. Все это выявляется в ходе проведения комплексных специальных проверок и специальных исследований.

Данные исследования и работы проводятся, как правило, при лицензировании деятельности организаций и сертификации технических средств и систем, предназначенных для обработки категорированной информации. Работы проводятся исследовательскими лабораториями и сертификационными центрами ФСТЭК РФ.

В ряде случаев, когда порядок работ не регламентирован нормативно-методическими документами, экономически целесообразней, не выявляя, сразу защитить (локализовать) каналы утечки, однако это относится только к естественным каналам.

5.1. Комплексные специальные проверки

Комплексная специальная проверка — это комплекс мероприятий, проводимых с использованием необходимых, в том числе и специализированных технических средств, направленных на исключение несанкционированного получения вероятным противником (злоумышленником) информации, содержащей сведения ограниченного доступа, с помощью внедренных в защищаемые технические средства и изделия специальных электронных закладочных устройств.

Целью проведения комплексных специальных проверок помещений является пресечение (предотвращение) получения злоумышленником (противником) защищаемой информации из этих помещений с помощью средств несанкционированного съема информации (НСИ). Тем самым предотвращается ущерб, который может быть нанесён собственнику, владельцу, пользователю защищаемой информации в случае использования злоумышленником (противником) этой информации в своих интересах. В процессе достижения целей комплексных специальных проверок решаются следующие задачи:

- выявление и нейтрализацию внедрённых противником закладочных устройств;
- выявление незакрытых потенциальных ТКУИ;
- определение мероприятий, требуемых для закрытия (ликвидации) выявленных потенциальных ТКУИ;

- сбор новых сведений о тактике применения противником средств НСИ и их характеристиках.

При проведении комплексных специальных проверок необходимо руководствоваться следующими принципами:

- соответствие положениям законов и других правовых актов, регулирующих отношения в области защиты информации (правозаконность);
- скрытность подготовки и выполнения работ;
- системность (периодичность) проведения;
- взаимосвязь с другими мероприятиями в общей системе защиты информации;
- комплексность применяемых методов и технических средств;
- достаточность проводимых работ для достоверной оценки защищённости помещений;
- комплексность разрабатываемых организационных, инженерных и технических мер защиты;
- достаточность рекомендуемых мер защиты для предотвращения утечки информации по выявленным потенциальным ТКУИ.

5.1.1. Порядок проведения комплексной специальной проверки

Проведение комплексной специальной проверки по выявлению специальных устройств перехвата (уничтожения) информации состоит из нескольких этапов.

Исключительно важную роль, оказывающую существенное влияние на весь ход и результаты проведения комплексной специальной проверки, играет подготовительный этап, поскольку качество подготовительных работ предопределяет надёжность результатов проверки. Часть работ этого этапа предполагает участие в них руководителя предприятия, на котором должна быть проведена проверка помещений. Поэтому от того, удастся ли с самого начала достичь взаимопонимания руководства предприятия и специалистов поисковой группы, в значительной степени зависит эффективность всех поисковых мероприятий.

В любом случае при организации и подготовке к проведению комплексной проверки основу составляет грамотно принятое решение.

Методика принятия управленческого решения была рассмотрена в третьей главе. В данном разделе рассмотрим конкретные вопросы, касающиеся принятия решения на проведение комплексной специальной проверки защищаемых помещений.

Принятие любого решения начинается с уяснения задачи и цели действий. Следующим этапом идет оценка обстановки, которая

проводится в три этапа: оценка противника, условий в которых придется решать стоящие задачи, для достижения цели и оценки своих возможностей. При этом в данном конкретном случае после оценки вероятного противника целесообразно начинать разработку замысла проведения проверки, что в дальнейшем позволит более качественно оценить свои возможности.

Уяснение задачи и цели действий. Суть проблемы в том, что защита информации — довольно дорогое занятие, требующее не только разовых, но и постоянных текущих затрат. Поэтому защищать необходимо только ту информацию, утечка которой может привести к экономическому, моральному или другому ущербу предприятию, организации, её руководству, отдельным сотрудникам предприятия или другим физическим лицам. Очевидно, что информация, отнесённая к категории защищаемой, может иметь различный характер и что утечка различной защищаемой информации может привести к разным последствиям. Поэтому необходимо знать не только, что и зачем надо защищать, но и насколько следует защитить конкретный вид охраняемых сведений. Это позволит дифференцировать мероприятия по обеспечению безопасности информации и тем самым сократить затраты на их проведение.

Однако необходимо отметить, что данное положение справедливо только для защищаемой информации, отнесенной руководством предприятия к сведениям, составляющих коммерческую тайну предприятия и включенных в перечень информации ограниченного доступа на предприятии. В отношении сведений, отнесенных к информации ограниченного доступа законодательно, меры защиты этих сведений определяются в соответствующих законодательных и нормативно-методических документах, выпускаемых соответствующими государственными органами. В этих документах определяется степень защиты определенного вида информации и основные мероприятия по реализации защиты.

Оценка обстановки. Львиная доля в оценке обстановки отводится оценке противника, ведь именно от того, насколько полно и качественно будет оценена противостоящая сторона, во многом будут зависеть и все последующие мероприятия. Нормативно-методические документы рекомендуют и требуют, чтобы в качестве противника при разработке плана комплексной проверки принимался наиболее подготовленный специалист. Однако при решении вопросов защиты конфиденциальной информации это не всегда представляется целесообразным и экономически выгодным. Ряд существующих организационно-методических документов по защите информации от несанкционированного доступа и технической разведки рекомендуют в качестве противника или нарушителя рассматривать субъекта, имеющего доступ

к работе на предприятии, являющегося специалистом высшей квалификации и знающего всё о работе предприятия и его системе безопасности, включая полные сведения о системе и средствах защиты информации. Эти рекомендации являются абсолютно правильными, когда речь идёт о защите секретов государства от любого вида посягательств, включая действия агентурной и технической разведки иностранных государств, однако, когда речь идет о защите информации конфиденциального характера, здесь необходимо рассматривать и применять несколько другой подход. Целесообразно рассмотреть несколько основных возможных ситуаций при оценке.

Анализ деятельности различных коммерческих структур позволяет сделать определенные выводы о том, что большинство руководителей принимают решение о проведении работ по выявлению различного рода ЗУ только после того, как понесены существенные потери за счет утечки информации. Как уже было сказано ранее, принятие решения и планирование работ по поиску ЗУ начинается с выявления побудительных мотивов. Таких мотивов может быть несколько. Рассмотрим наиболее вероятные ситуации, когда руководитель фирмы может принять решение на проведение поисковых работ по выявлению ЗУ.

Более подробно рассмотрим каждую ситуацию с целью определения комплекса необходимых мероприятий для защиты от утечки информации в каждом конкретном случае.

Первая ситуация. Вариант, когда на фирме планируется проведение плановой проверки с целью выявления и закрытия возможных потенциальных технических каналов утечки информации. Этот случай можно считать наиболее сложным, ибо он предполагает в качестве вероятного противника широкий круг лиц, это могут быть: конкурирующие предприятия, разного рода криминальные элементы и структуры, неразборчивые в средствах представители органов массовой информации, имиджевые и иные фирмы, занимающиеся сбором компромата по заказу заинтересованных лиц. Вашим противником могут оказаться организации, поддерживающие с вами деловые отношения, и отдельные личности.

При определении круга ваших вероятных противников следует помнить, что они могут иметь самые разнообразные побудительные мотивы для внедрения на вашем предприятии средств НСИ. Перехват вашей защищаемой информации может, например, проводиться с целью:

- анализа вашей деятельности, чтобы проверить вашу кредитоспособность или избежать деловых отношений с возможно недобросовестным партнёром;

- пресечения возможно планируемого вами, но невыгодного для себя действия своим упреждающим действием (преднамеренного срыва сделок и иных соглашений);
- последующей продажи собранной информации конкурентам, заинтересованным лицам или организациям;
- последующего шантажа вас угрозой разглашения собранной информации, передачи её конкурентам или заинтересованным лицам;
- разглашения собранной информации с целью заставить вашего конкурента совершить выгодные для себя действия и т. д.

Как мы видим, данный вариант с точки зрения предполагаемых угроз наиболее опасный. Следовательно, подготовка и проведение поисковых работ должна охватывать все аспекты и проводиться в полном объёме. Так как этот вариант наиболее объёмный и охватывает практически все виды поисковых работ, то в дальнейшем все основные поисковые мероприятия будут рассматриваться применительно к нему.

Вторая ситуация. Вариант, когда в результате утечки информации конфиденциального характера, которой владело ограниченное число доверенных лиц фирмы, нанесён существенный финансовый ущерб. В данном случае прежде всего необходимо наиболее тщательно проанализировать сложившуюся ситуацию с целью определения, каким образом и в какой период времени ваша информация могла попасть злоумышленникам. Первым шагом в данной ситуации должно быть определение, как данная информация обрабатывалась и циркулировала на вашем предприятии. Необходимо определить возможные, наиболее вероятные каналы её утечки. При этом особое внимание необходимо уделить анализу лиц, владевших данной информацией, и оценке возможности утечки информации через них.

Далее необходимо выяснить, какие нестандартные ситуации были в этот период времени. Такими ситуациями могут быть: неожиданный выход из строя системы энергоснабжения, связи, нарушение функционирования систем коммуникации и т. д. То есть ситуаций, требующих появления на фирме посторонних лиц. Если подобные ситуации случались в этот период, то следующим шагом должен быть детальный анализ действий данного лица во время нахождения на территории предприятия. Прежде всего необходимо выяснить бесконтрольное время пребывания данного человека на фирме. Определить, в какие помещения фирмы в этот период времени он мог попасть.

Исходя из ответов на поставленные вопросы будут планироваться и мероприятия по проведению поисков. Так, если данное лицо имело доступ в ЗП и находилось там бесконтрольно в течение нескольких

минут, то особое внимание необходимо обратить на телефонную аппаратуру (возможна замена трубки). При осмотре ЗП необходимо выявить вновь появившиеся предметы интерьера и другие посторонние вещи (канцелярские принадлежности, предметы неустановленного назначения, посторонние сотовые телефоны и т. д.). Далее необходимо осмотреть скрытые полости, пригодные для установки в них ЗУ.

При отсутствии в данный период времени посторонних лиц возникает ситуация, когда придется детально анализировать круг лиц фирмы, имевших доступ к перехваченной информации. При этом анализ необходимо начинать с выяснения того, каким образом стало известно об утечке информации, где и в каком виде она появилась, кто и с какой целью ей воспользовался.

После получения ответов на эти вопросы необходимо выяснить, кто из лиц вашей фирмы, владевших данной информацией или имевших доступ в помещение, где она циркулировала и обрабатывалась, имел какое-либо отношение к фирме, воспользовавшейся вашей информацией. Выявление таких лиц приведет к сужению круга подозреваемых, а следовательно, и к более целенаправленному проведению комплекса дальнейших мероприятий.

Третья ситуация. Вариант, связанный с переездом фирмы в новый офис. В данной ситуации прежде всего необходимо проанализировать, к какому классу относится новый офис. Здесь возможно несколько вариантов: это может быть новое офисное здание, целиком планируемое под фирму, это может быть несколько помещений в новом офисном центре, а может быть занятие помещений, ранее арендуемых другой фирмой.

В принципе, перечень необходимых проверочных мероприятий во всех случаях, как правило, одинаков и будет отличаться только глубиной проводимых поисковых мероприятий. При этом прежде всего необходимо определиться с помещениями, которые будут относиться к разряду категорированных, и в зависимости от категории информации, планируемой для обработки, оценить пригодность данных помещений. Если помещение признано пригодным для обработки информации ограниченного пользования, необходимо определить и назначить специалиста, ответственного за данное помещение, который в дальнейшем должен полностью контролировать проведение всех работ, и всех лиц, посещающих данное помещение. До размещения в этом помещении офисной мебели, предметов интерьера и электронного оборудования необходимо принять меры по защите данного помещения от физического проникновения посторонних лиц, подключить систему сигнализации и обеспечить сдачу помещения под охрану.

После решения вопросов организационно-режимного характера можно приступать к решению вопросов технической проверки данного

помещения на наличие различного рода закладочных устройств. При этом проверку целесообразно начинать с обследования ограждающих конструкций помещения на наличие различного рода специальных технических средств, возможно внедренных в ограждающие конструкции. Проверку целесообразно проводить с помощью нелинейного локатора. Методика работы с данным прибором частично рассматривалась во 2-й главе и более подробно будет рассмотрена в дальнейшем.

После проверки ограждающих конструкций можно заниматься комплектацией защищаемого помещения. Комплектация необходимой мебелью, оборудованием и предметами интерьера должна производиться под контролем ответственного за данное помещение сотрудника фирмы. Все комплектующие компоненты защищаемого помещения должны быть проверены на наличие закладочных устройств и недекларированных возможностей. Вся мебель, оборудование и предметы интерьера защищаемого помещения должны быть промаркированы и учтены в соответствующем журнале ограниченного доступа. Их местоположение должно быть зафиксировано с помощью цифрового фотоаппарата. Фото расположения мебели, оборудования и предметов интерьера должно храниться в качестве приложения в журнале учета.

Четвертая ситуация. Вариант, когда проводится профилактическая проверка перед проведением важных мероприятий. В этой ситуации масштаб и номенклатура поисковых мероприятий будут зависеть от многих факторов и прежде всего от оценки важности проводимого мероприятия, интереса конкурентов к тематике проводимого мероприятия и, как следствие, оценке степени угроз безопасности информации.

При оценке угроз необходимо прежде всего оценить состояние защиты речевой информации на защищаемом объекте, состояние технических средств обработки и преобразования речевой информации, планируемых для использования в ходе проведения мероприятия. Далее необходимо оценить состояние организационно-режимных мер по контролю доступа в защищаемое помещение, в котором планируется проведение важного мероприятия. Наличие и принадлежность помещений, смежных с ЗП. Оцениваются возможности доступа в смежные помещения посторонних лиц и установки в них технических средств несанкционированного съема информации (электронных стетоскопов, виброметров, акустических микрофонов). При выходе ограждающих конструкций ЗП на неохраняемую территорию визуальным осмотром необходимо убедиться в отсутствии на стеновой панели и под карнизами оконных проемов посторонних предметов. Необходимо продумать возможности по ограничению проноса в ЗП электронной техники, которая может использоваться для перехвата, накопления и передачи

речевой информации. Непосредственно перед проведением важного мероприятия необходимо провести анализ состояния радиоэлектронной обстановки в ЗП. Радиомониторинг целесообразно провести в течение суток. При обнаружении неизвестных источников радиоэлектронного излучения определить их принадлежность и местоположение.

Непосредственно перед проведением мероприятия должна быть обеспечена невозможность проноса в ЗП электронных устройств (сотовых телефонов, диктофонов и радиомикрофонов). Для этого необходимо использовать все допустимые меры, как организационно-режимные, так и технические. Однако необходимо отметить, что все проводимые мероприятия не могут полностью гарантировать отсутствие в ЗП средств несанкционированного получения информации. Следовательно, должна быть предусмотрена возможность технической защиты и оперативного блокирования несанкционированных излучений из ЗП непосредственно в ходе проведения мероприятия. В процессе проведения мероприятия специалистами технической защиты информации должен проводиться текущий контроль состояния радиоэлектронной обстановки в ЗП с целью выявления вновь появившихся в ходе совещания источников радиоэлектронного излучения из ЗП. При этом должна быть предусмотрена возможность активного подавления источников несанкционированного излучения из ЗП с использованием генераторов прицельной помехи. С этой целью специалисты в области защиты информации должны проводить анализ текущей радиоэлектронной обстановки в ходе проведения мероприятия. Сделать это можно только при развернутом в ЗП аппаратно-программном комплексе, позволяющем осуществлять постоянный анализ текущей радиоэлектронной обстановки в режиме онлайн. Такой анализ позволит в режиме реального времени определить выход в эфир несанкционированного источника радиоэлектронного излучения и своевременно поставить помеху на частоте излучения, что предотвратит утечку информации в период проведения совещания.

После разработки модели вероятного противника целесообразно сразу перейти к выработке замысла проведения специальной проверки помещений. Это в дальнейшем позволит более качественно оценить условия и свои возможности по организации противодействия.

Разработку замысла проведения специальной проверки помещений можно считать наиболее важным элементом работ подготовительного этапа.

По определению замысел — это основная идея, раскрывающая состав, содержание, взаимосвязь и последовательность осуществления технических и организационных мероприятий, необходимых для достижения цели проверки. В состав замысла входят:

- целевая установка, раскрывающая для противодействия какому противнику будут проводиться поисковые мероприятия;
- масштаб и место проведения поисковых мероприятий;
- время проведения проверки;
- легенда(ы), под прикрытием которой будет проводиться специальная проверка;
- как активировать внедренные средства НСИ;
- варианты действий в случае обнаружения средств НСИ.

Целевая установка непосредственно вытекает из результатов работы по выявлению или уточнению вероятного противника и его возможностей. Результаты оценки финансовых, оперативных и технических возможностей противника предопределяют также масштаб проведения поисковых мероприятий. При этом под масштабом здесь следует понимать не только количество и общую площадь помещений, которые вы намечаете для специальной проверки, но и глубину поисковых, а также сопутствующих исследований и их номенклатуру. Чем большими финансовыми и техническими возможностями обладает ваш вероятный противник, тем более тщательными и разносторонними должны быть поисковые работы и работы по исследованию потенциальных ТКУИ.

Очень важным элементом на подготовительном этапе является выбор времени проведения проверки, а именно в рабочий или выходной день, днём или ночью, в рабочее время или до начала рабочего времени, а может быть сразу по окончании рабочего дня. При этом важно знать, что при проведении проверки в нерабочее время большинство закладочных устройств, особенно дистанционного управления, будут отключены, что не гарантирует выполнение поставленной задачи.

Кроме того, необходимо отметить, что выбор времени проведения проверки непосредственно связан с разработкой легенд, под прикрытием которых будет работать поисковая бригада, так как одним из основополагающих принципов проведения комплексных специальных проверок помещений является скрытность выполнения основных поисковых работ.

Из этого вытекает необходимость разработки для персонала предприятия и посетителей, в том числе лиц, возможно, работающих на противника, правдоподобной версии (легенды прикрытия) появления на предприятии специалистов, занимающихся проведением измерительных и поисковых работ с использованием сложного и довольно специфического оборудования.

При выборе времени проведения проверки необходимо заранее продумать меры по активации средств НСИ. Можно, например, заранее распространить среди сотрудников предприятия информацию

о якобы намеченном на выбранное для проверки время важном совещании с приглашением лиц из сторонних организаций. Ещё лучше, если руководство предприятия и в самом деле проведёт фиктивное, но правдоподобное совещание, способное настолько заинтересовать вероятного противника, что он активизирует все, включая дистанционно управляемые, средства НСИ. Очевидно, что выбранный сценарий мер по активации внедренных средств НСИ не должен противоречить легенде прикрытия поисковых мероприятий.

Разрабатываемые легенды прикрытия должны легко вписываться в деятельность предприятия и оказывать минимальное деструктивное влияние на его повседневную деятельность. Весьма вероятно, что придётся разрабатывать не одну, а сразу несколько легенд прикрытия, в том числе для появления на предприятии одного или нескольких членов поисковой бригады, имеющих задачу провести предварительный осмотр помещений. Для каждой из легенд должны быть разработаны способы и определено время их доведения до персонала предприятия, составлен перечень необходимых для подтверждения легенды оборудования, приборов и документов. Общими требованиями к создаваемым легендам прикрытия являются их правдоподобность, естественность, надёжность и соответствие создаваемой ситуации содержанию работ членов поисковой бригады.

В качестве примера приведем несколько, наиболее приемлемых, на наш взгляд, вариантов легенд:

- проверку специалистами телефонного узла связи состояния телефонных линий и оборудования;
- проверку состояния отопительной системы, водопроводных и других инженерно-технических коммуникаций, проведение на них ремонтных работ;
- плановую проверку функционирования систем охранной и пожарной сигнализации;
- проведение регламентных работ на элементах системы внутренней связи предприятия;
- проверку системы заземления, состояния электроизоляции проводов системы освещения, элементов системы электропитания;
- поиск местонахождения искрящих контактов скрытой электропроводки для устранения помех ПЭВМ;
- проверку приглашёнными экологами состояния окружающей среды (освещённости рабочих мест, уровня радиации и электромагнитных излучений, состава воздуха и т. п.);
- подготовку и проведение косметического ремонта помещений.

Рассмотренные вопросы замысла в полной мере лежат в компетенции руководителя предприятия, так как их важность для успеха

проверки, их тесная взаимосвязь и влияние на обычный порядок работы предприятия, а также необходимость проработки этих вопросов в едином пакете требуют решений, принимать которые необходимо самому руководителю предприятия.

Если проверка производится собственными силами соответствующих служб предприятия, то некоторые вопросы им будут известны по роду своей деятельности и объем предварительной работы будет несколько меньшим.

Для более полного представления характера и объема необходимых работ мы будем рассматривать вопросы организации и проведения комплексной специальной проверки применительно к её проведению внешней организацией.

Как правило, руководители предприятия стремится переложить решение вопросов замысла на руководителя службы безопасности. Однако подчеркнем необходимость личного участия руководителя предприятия в разработке плана проведения проверки. Это обусловлено прежде всего важностью всех этих вопросов для успеха проверки, их тесной взаимосвязью, влиянием на обычный порядок работы предприятия и необходимостью проработки в едином пакете. Все это требует решений, принимать которые необходимо самому руководителю предприятия, так как именно руководитель предприятия наиболее полно представляет себе:

- откуда может исходить угроза его секретам;
- какая легенда прикрытия работ по проверке помещений наиболее органично впишется в деятельность предприятия;
- какой, не противоречащий легенде сценарий мер по активации средств НСИ следует предпочесть.

Перед заключением договора на проведение комплексной специальной проверки специалисты, которые будут проводить проверку должны изучить и сделать предварительный осмотр объектов проверки. При этом основное внимание должно быть уделено:

- знакомству с профилем предприятия, особенностями его функционирования, назначением и особенностями использования подлежащих проверке помещений;
- изучению имеющихся планов территории предприятия, окружающей застройки, размещения на территории предприятия зданий и сооружений, размещения в зданиях помещений, подлежащих проверке и смежных с ними;
- изучению имеющихся на предприятии планов и строительных чертежей, подлежащих проверке и смежных с ними помещений, другой строительной и ремонтной документации на эти помещения;
- знакомству с организацией охраны территории предприятия, зданий и проверяемых помещений, изучению порядка и системы кон-

троля доступа на территорию предприятия, в подлежащие проверке и смежные с ними помещения;

- изучению схем инженерно-технических коммуникаций, энергоснабжения, связи, охранной, пожарной сигнализации, других документов, относящихся к работам по прокладке, ремонту и демонтажу проводных и инженерно-технических коммуникаций в подлежащих проверке и смежных с ними помещениях, обработке защищаемой информации в проверяемых помещениях;
- знакомству со сложившейся на предприятии системой защиты информации, используемыми техническими средствами защиты информации и мерами, принятыми по предотвращению утечки информации из подлежащих проверке помещений.

В ходе предварительного осмотра целесообразно особое внимание обратить на:

- конструктивные особенности проверяемых помещений и инженерно-технических коммуникаций, не отражённые в предварительно изученных документах (подшивные или подвесные потолки, подшивные стены, фальшполы, наличие подпольных каналов, плинтусов, съёмных панелей, наружных и скрытых кабельных каналов, трубопроводов, защитных экранов и т. п.);
- места возможного доступа посторонних лиц к элементам ограждающих конструкций помещений, технологическим и проводным коммуникациям, проходящим через подлежащие проверке помещения;
- следы недавно проведённого ремонта, реконструкции или вторжения в элементы ограждающих конструкций, инженерно-технических и проводных коммуникаций;
- особенности прокладки проводных коммуникаций, наличие линий, транзитом проходящих через проверяемые помещения;
- особенности внутреннего убранства и обстановки помещений (характер отделки стен, наличие напольных покрытий, количество мебели и её простота, количество и сложность предметов интерьера и т. д.).

Одним из важных вопросов в изучении объекта поиска и его окружения является получение материалов о вероятном противнике, его профессиональных и технических возможностях. Получение материалов о вероятном противнике должно начинаться с подробной беседы с руководителем организации объекта поиска. Особое внимание при этом необходимо уделить конкретизации как конфиденциальных сведений, так и направлениям деятельности, которые могут представлять интерес для конкурирующей организации, на основе чего целесообразно очертить возможные каналы прогнозируемой утечки информации

и отработать предварительный план по проведению поисковых исследований.

Для разработки конкретного плана проведения поисковых мероприятий (гласно или негласно) различными путями добывается информация о вероятном «противнике» и необходимая информация для последующих исследований. При этом особое место в изучении объекта поиска и его окружения занимает получение информации:

- по ведению делопроизводства на объекте поиска;
- по порядку прохождения информации конфиденциального характера как внутри организации объекта поиска, так и за её пределами;
- по режиму работы организации и посещения её посторонними сотрудниками, в том числе и возможного посещения сотрудниками прогнозируемого противника, по взаимодействию сотрудников внутри организации и сотрудников других фирм и по другим вопросам, изучение которых будет способствовать оперативному, скрытному и эффективному проведению поисковых исследований.

Необходимо изучить, когда и как проводился косметический и капитальный ремонт, монтаж и демонтаж проводных и трубопроводных коммуникаций, замена мебели, перестановка предметов быта и интерьера.

Кроме этого, необходимо получить данные о наличии в проверяемых помещениях сувениров, подарков и других предметов от сотрудников других организаций, а также о том, каким образом осуществляется покупка мебели, картин, радиоаппаратуры и т. п. для этих помещений.

В зависимости от полученной информации, особенно касающейся вероятного противника, его технического и профессионального состояния, о его намерении добывать информацию, а именно однократного получения информации конфиденциального характера или её многократного получения, планируется и направленность поисковых работ:

- «одноразовые» закладочные устройства (далее ЗУ) могут размещаются в каких-либо предметах бытового назначения и интерьера: в радио-, теле- и другой аппаратуре, в предметах интерьера и в других предметах. Как правило, основное назначение данных бытовых приборов сохраняется. При этом они не должны бросаться в глаза работникам предприятия и могут быть внесены на объект поиска при проведении каких-либо текущих ремонтных работ или посетителями. Питание этого вида ЗУ обеспечивается от автономного источника (батареи или аккумулятора), а в некоторых случаях может быть использовано питание от линии электросети или телефонной линии;

- долговременные или «многократные» ЗУ, как правило, стационарно внедряются в элементы строительных конструкций (стены, пол, потолочные перекрытия, вентиляционный канал и т. д.) в ходе проведения реконструкции или капитального ремонта защищаемых помещений. ЗУ могут быть внедрены в элементы абонентской телефонной сети (аппарат, розетку, телефонный шкаф и т. д.), в электросеть (розетка, подрозетник и т. д.) и в элементы других проводных коммуникаций, а также в элементы предметов быта и интерьера с обеспечением их питания от линии электросети, при проведении ремонтных или профилактических работ, проводимых специалистами внешних ремонтных организаций.

Необходимо отметить, что при «одноразовой» добыче конфиденциальной информации наиболее вероятным каналом передачи негласно добытой информации является радиоканал. В этом случае питание ЗУ, как правило, осуществляется от автономного источника тока (батарей или аккумуляторов).

При «многократной» добыче информации, как правило, осуществляется стационарное внедрение на объекте разведки ЗУ, а в качестве канала передачи сигналов информации могут быть использованы закамуфлировано проложенная проводная линия, абонентская телефонная линия, линия электросети и другие проводные коммуникации. Питание таких ЗУ, чаще всего, осуществляется от электросети.

Наряду с этим в качестве каналов передачи сигналов информации могут быть использованы элементы строительных конструкций (пол, стены, потолочные перекрытия, водопроводные трубы, оконные стекла и т. д.). В этом случае ЗУ, в основном, размещаются на пункте приёма и обработки сигналов, который, как правило, устанавливается за пределами помещений объекта поиска.

Вышеперечисленные особенности при негласном получении информации должны быть учтены при изучении объекта проверки и его окружения.

В результате у специалистов поисковой бригады должно сложиться ясное представление:

- о характере окружающей застройки и прилегающей местности;
- конструктивных и других особенностях здания, проверяемых и смежных с ними помещений;
- размещённом в них оборудовании, прохождении в проверяемых и смежных с ними помещениях проводных и инженерно-технических коммуникаций;
- доступности помещений для посетителей и персонала предприятия, системах охраны, контроля доступа и защиты информации.

Этих представлений должно быть достаточно для составления перечня поисковых и исследовательских работ, перечня необходимой

для этих работ аппаратуры и ориентировочной оценки ожидаемых трудозатрат на их выполнение.

После предварительного осмотра необходимо осуществить предварительное распределение сил и средств, которое в дальнейшем позволит определить оптимальный состав поисковой группы и общее время проверки. При этом тщательно продуманный сетевой график позволит согласовать, в рамках единой структуры, процесс проведения всех требуемых поисковых и исследовательских работ с учётом их объёма и взаимовлияющих ограничений.

Целесообразен следующий порядок действий:

- определяются ориентировочные затраты времени для выполнения каждой из запланированных работ, в том числе ожидаемая продолжительность работ с каждым из видов поисковой и исследовательской аппаратуры;
- среди этих работ выделяются такие, одновременное проведение которых невозможно из-за их взаимоисключающего влияния или других соображений;
- суммированием определяются затраты времени, необходимые для последовательного выполнения работ, одновременное проведение которых невозможно;
- отмечаются затраты времени на наиболее трудоёмкую из числа оставшихся работ;
- определяется минимально возможная продолжительность непосредственного проведения специальной проверки как наибольшая величина из затрат времени, определённых в двух предыдущих пунктах;
- в пределах минимально возможной продолжительности непосредственного проведения специальной проверки распределяются все запланированные работы таким образом, чтобы минимизировать количество одновременно (параллельно) выполняемых работ.

После проведения предварительного осмотра, определения времени проведения проверки и состава бригады переходят к составлению плана проведения комплексной специальной проверки. План проведения комплексной специальной проверки помещений является генеральным документом, в котором определяются масштаб, конкретное содержание и методика проведения проверки. Если все изложенные в предыдущих разделах работы подготовительного этапа выполнены с требуемой тщательностью, составление и оформление этого плана не вызывает каких-либо трудностей.

Вариант структуры типового плана проведения комплексной специальной проверки помещений представлен далее.

Первый раздел плана включает выводы из оценки противника.

Во второй раздел входит замысел проведения комплексной специальной проверки помещений, включающий:

- цель (побудительный мотив) проведения проверки;
- перечень и краткую характеристику проверяемых помещений;
- перечень запланированных поисковых работ и исследований;
- время проведения проверки;
- легенды, под прикрытием которых будет проводиться проверка;
- меры по активизации внедренных средств НСИ;
- действия в случае обнаружения средств НСИ.

В третьем разделе плана определяются привлекаемые силы и средства, их распределение по объектам и видам состав поисковой бригады, а именно:

- привлекаемые для проведения проверки технические средства и основные особенности их применения, определяемые условиями проверки;
- определение количественного состава сил;
- распределение сил и средств по объектам и видам работ;
- дополнительные меры по активизации внедренных средств НСИ.

Четвертый раздел плана посвящен перечню подготавливаемых по результатам проверки итоговых и отчетных документов и срокам их представления для утверждения.

План оформляется в виде текстуального документа, с необходимыми таблицами и поясняющими схемами.

Ознакомившись со структурой плана проведения комплексной специальной проверки помещений, более детально рассмотрим каждый раздел плана.

В разделе *выводов из оценки противника* целесообразно указать:

- категорию лиц, к которым может принадлежать субъект, выбранный вероятным противником для внедрения средств НСИ и съёма информации;
- возможный уровень знаний, навыков и квалификации субъекта, осуществляющего внедрение средств НСИ;
- возможные виды применяемых средств НСИ, ожидаемая степень соответствия их характеристик наиболее продвинутым образцам аналогичных средств;
- возможные способы, время установки (внедрения) средств НСИ и действий по съёму информации;
- вероятные действия в случаях установления намерений провести специальную проверку помещений, факта проведения такой проверки и факта обнаружения внедрённых средств НСИ.

В *замысле проведения комплексной специальной проверки помещений* целесообразно отразить следующие вопросы:

- цель (побудительный мотив) проведения специальной проверки помещений;
- оформленный в виде таблицы или текстуально перечень проверяемых помещений с краткой характеристикой каждого помещения, а именно: назначение, площадь и объём, особенности конструкции, основные виды обстановки, установленного оборудования и процент занимаемой ими общей площади (объёма) помещения, виды проводных и технологических коммуникаций;
- перечень запланированных для каждого помещения поисковых работ и сопутствующих исследований (включая работы, намеченные к проведению в смежных помещениях и на наружных поверхностях ограждающих строительных конструкций) с указанием их ожидаемой трудоёмкости;
- время проведения специальной проверки помещений: дата, начало, конец, общая продолжительность непосредственного проведения проверки;
- содержание и время действия легенды или нескольких легенд, под прикрытием которых будут проводиться работы по специальной проверке помещений, способы и начало доведения легенд до персонала предприятия, перечень оборудования и документов, необходимых для подтверждения легенд;
- меры по активации внедренных средств НСИ, способы и начало их выполнения;
- действия поисковой бригады в случае обнаружения средств НСИ.

В разделе *привлекаемые силы и средства* прежде всего рассматриваются вопросы:

- количественный и персональный состав поисковой бригады;
- перечень специального оборудования и технических средств, привлекаемых для проведения специальной проверки помещений с указанием основных особенностей их применения в рамках выбранных легенд прикрытия и других ограничений, налагаемых условиями проверки;
- сетевой график выполнения запланированных поисковых и исследовательских работ или таблицу распределения специалистов поисковой бригады, оборудования и технических средств по видам работ и объектам специальной проверки;
- текстуальную часть с изложением дополнительных мер по активизации внедренных средств НСИ в процессе применения конкретных типов поисковой аппаратуры.

Четвертый, заключительный раздел плана проведения комплексной специальной проверки помещений должен содержать перечень подготавливаемых по результатам проверки итоговых и отчётных до-

кументов и срок их представления для утверждения. В этот перечень могут входить:

- акт проведения комплексной специальной проверки помещений;
- описание проведённых работ и исследований;
- протоколы измерений;
- рекомендации по повышению надёжности защиты информации от её возможной утечки по техническим каналам;
- другие документы.

Разработанный план утверждается руководителем предприятия и после утверждения становится документом обязательным для исполнения.

После утверждения плана проверки группа может приступить к непосредственной проверке.

5.1.2. Выполнение поисковых мероприятий

Рассмотрим вариант проведения поисковых мероприятий непосредственно на объекте.

Первым этапом проводятся исследования, которые условно можно разделить на четыре вида:

- радиомониторинг;
- осмотр помещения;
- обследование электрических и электронных приборов;
- проверка проводных коммуникаций.

Для их выполнения используют: специальные радиоприёмные устройства, программно-аппаратные комплексы, металлодетекторы, нелинейные локаторы, индикаторы электромагнитного поля, сканирующие приемники и радиочастотомеры, переносные рентгеновские и тепловизионные приборы, и прочие имеющиеся в наличии поисковые средства. Досмотр труднодоступных позиций осуществляют с применением зеркал или различных эндоскопов.

Радиомониторинг. Основная задача радиомониторинга заключается в проведении предварительного анализа радиоэлектронной обстановки с целью составления карты (базы) загрузки радиоэфира в конкретном районе проведения проверки и обнаружении неизвестных и несанкционированных излучений.

Предварительный сбор данных и анализ радиоэлектронной обстановки заключается в выявлении радиоизлучений, превышающих пороговое значение, в районе проверяемых помещений, определении принадлежности обнаруженных радиоизлучений и их предварительной сортировке для последующего специального тестирования и анализа на принадлежность к излучениям средств НСИ и ПЭМИ средств оргтехники из проверяемых помещений.

По согласованию с руководством предприятия дополнительными задачами анализа радиоэлектронной обстановки на этом этапе могут быть контроль соблюдения сотрудниками предприятия установленных его руководством ограничений на использование открытых каналов радиосвязи, контроль и оценка эффективности используемых технических средств защиты информации и другие задачи.

Методика предварительного сбора данных радиоэлектронной обстановки и их анализа во многом определяется типами используемой аппаратуры. Хотя порядок подключения и настройки аппаратуры будет различен, можно однозначно определить общий подход и алгоритм проведения предварительного радиомониторинга.

В настоящее время наиболее целесообразно для ведения радиоконтроля и выявления радиоизлучающих средств НСИ использовать автоматизированные аппаратно-программные комплексы, выполненные на базе ПЭВМ и сканирующего радиоприёмника. В современных условиях наиболее оптимальным является проведение круглосуточного радиомониторинга в течение одной недели с применением автоматизированного аппаратно-программного комплекса. Применение такого комплекса позволяет:

- в автоматическом режиме снять панораму загрузки радиодиапазона;
- с минимальным участием оператора идентифицировать принимаемые излучения с сигналами известных источников (например, радиовещательных станций, систем телефонной сотовой или транкинговой связи);
- провести ручной анализ остальных сигналов по их спектральным и другим характеристикам;
- составить списки частот идентифицированных излучений и частот «подозрительных» сигналов.

Примерный алгоритм проведения предварительного радиомониторинга выглядит следующим образом:

- определяется уровень шумов в районе контроля;
- выбираются пороговые значения для проверяемого частотного диапазона (как правило, превышение порога над уровнем шума 5...15 дБ).
- выбирается режим работы комплекса (наиболее целесообразно использовать круглосуточный радиомониторинг в течение недели с захватом выходных дней).

Активное развитие мобильных аппаратно-программных комплексов, приближение их возможностей к стационарным и применение современного программного обеспечения позволило оптимизировать методику проведения предварительного радиомониторинга и сущест-

венно облегчить анализ исходной обстановки в контролируемом помещении. Наиболее целесообразен следующий порядок работы.

В районе контролируемых помещений там, где гарантированно отсутствуют закладочные устройства, снимается исходная радиоэлектронная обстановка (радиомониторинг в течение нескольких часов в рабочее время, на удалении от объектов проверки на 300...500 м, но не более одного километра). В полученной спектрограмме радиоэлектронной обстановки гарантированно отсутствуют сигналы от ЗУ, передающих информацию по радиоканалу, так как:

- во-первых, средний радиус действия ЗУ 250...350 м, что гарантирует невозможность получение информации из защищаемых помещений;
- во-вторых, злоумышленник не может знать, как и где будет сниматься исходная обстановка.

Таким образом, полученная обстановка, априори, будет состоять только из сигналов легальных источников и случайных помеховых сигналов. Сигналы анализируются и по возможности удаляются с монитора случайные помеховые сигналы.

После анализа аппаратно-программный комплекс разворачивается для радиомониторинга проверяемых помещений.

Наиболее оптимальным на этом этапе будет следующий порядок работы:

- по согласованию с руководством предприятия определяется время начала, режим и продолжительность работы временного пункта радиоконтроля, место его развёртывания, перечень решаемых задач, легенда прикрытия работы;
- проводится необходимая подготовка аппаратуры для развёртывания и работы временного пункта радиоконтроля.

В запланированное время временный пункт радиоконтроля развёртывается и приступает к работе.

С использованием автоматизированного аппаратно-программного комплекса осуществляется последовательный просмотр и анализ реальной радиоэлектронной обстановки в помещениях, подлежащих проверке. Выявляются и анализируются особенности принимаемых сигналов. Применяя метод вычитания спектра, оператор существенно сокращает время для анализа полученной исходной радиоэлектронной обстановки, так как на экране монитора останутся только сигналы, передаваемые из контролируемых или смежных с контролирумыми помещений. Это могут быть легальные сигналы и сигналы неизвестного происхождения. Полученная обстановка анализируется с целью определения источников излучения. Определяется принадлежность оставшихся сигналов к легальным источникам излучений и выявляются нелегальные.

Частоты сигналов, принадлежность которых выяснить не удалось или которые идентифицируются с сигналами средств НСИ, остаются на экране монитора для последующего наблюдения за ними и дополнительного анализа.

Периодически проводится повторный просмотр загрузки диапазонов для выявления и анализа новых излучений. Ежедневно за 1...1,5 часа до начала работы фирмы и через 1...1,5 часа после окончания работы целесообразно проанализировать состояние радиоэлектронной обстановки.

В промежутках между повторными просмотрами загрузки диапазонов осуществляется постоянный или периодический контроль оставленных на мониторе «подозрительных» частот с контролем на регистрирующей аппаратуре проходящей информации и фиксацией времени начала и окончания работы источников излучений.

По истечении времени, отведённого для предварительного сбора данных и анализа радиоэлектронной обстановки, временный пункт радиоконтроля свёртывается.

В удобном месте, но не на глазах сотрудников предприятия, оператор по результатам работы приёмо-анализирующей и документирующей аппаратуры проводит дополнительный анализ накопленных данных, уточняет список «подозрительных» частот. Выводы, полученные в результате данного анализа, позволят определить объём и методику предстоящей работы в ходе непосредственного проведения специальной проверки помещений.

Таблица занятости частот в аппаратно-программных комплексах выводится в электронном виде на экран ПЭВМ. Форма таблицы позволяет легко уточнять и упорядочивать данные, вставлять в соответствующие места таблицы необходимое количество дополнительных строк при появлении новых сигналов и источников радиоизлучений.

В современных условиях целесообразно проведение круглосуточного радиомониторинга. В этом случае полученные данные позволят выявить появляющиеся в эфире излучения с началом и в течение работы предприятия. Целесообразно провести анализ данных контроля радиодиапазона за один–два часа до начала рабочего дня на предприятии и через один–два часа после окончания рабочего дня и убытия с предприятия его руководства.

Организацию предварительного радиомониторинга, порядок применения и методику анализа полученной информации рассмотрим на примере работы комплексов «Спектр-МК» и его дальнейшего развития и модификации «Спектр-Professional».

Данные рекомендации разработаны для повышения эффективности использования комплексов радиоконтроля при решении задач

обнаружения сигналов несанкционированных передатчиков специальных технических средств (СТС) (радиомикрофонов, беспроводных видеокамер и т. п.). Они содержат общие алгоритмы обнаружения и распознавания типовых сигналов закладочных устройств, а также расширяют и дополняют инструкцию по эксплуатации комплекса в части практических значений величин и порогов, используемых при настройке фильтров-классификаторов. Рекомендации позволят более полно и эффективно использовать широкие возможности комплекса при проведении радиомониторинга и поисковых мероприятий.

Все алгоритмы носят рекомендательный характер и не должны рассматриваться как жесткие правила. Пользователям необходимо самостоятельно оценивать обстановку и необходимость использования того или иного алгоритма. Рекомендации разработаны с учетом интерфейсных особенностей и аппаратных возможностей комплекса «Спектр-МК», «Спектр-Professional» и не могут быть эффективно использованы при работе с другой радиоприемной аппаратурой.

Калибровка комплекса. Калибровку комплекса необходимо проводить перед вводом изделия в эксплуатацию или при замене одного из блоков входящих в состав комплекса. Целью калибровки является исключение из процесса анализа собственных шумов радиоэлектронной аппаратуры, входящей в состав комплекса.

Порядок калибровки:

1. Отключить антенны от антенных входов коммутатора.

2. Выбрать в интерфейсе программного обеспечения (ПО) в закладке УСТРОЙСТВА меню НАСТРОЙКИ число каналов — 3.

3. Запустить комплекс на сканирование во всем диапазоне частот.

4. По окончании 1–2 циклов процедуру сканирования принудительно завершить.

5. Установить значение порога обнаружения выше естественного радиошума на 10 дБ*.

6. В закладке ФИЛЬТРЫ меню НАСТРОЙКИ установить значение превышения порога [+ дБ] — 15 дБ*.

7. Запустить комплекс на сканирование в диапазоне частот (40... ...3000 МГц).

8. По окончании 10 циклов процедуру сканирования принудительно завершить.

9. Сохранить обнаруженные сигналы в файле Spurios с соответствующими комментариями (формат: начальная частота, конечная частота, примечание).

Примечание. * — указанные величины являются рекомендуемыми и могут изменяться в зависимости от окружающей электромагнитной обстановки.

Таблица 5.1

Вид модуляции	Ширина спектра	Возможный источник
AM	9...12 кГц	Радиостанции гражданской и военной авиации
WFM (FM)	150...200 кГц	Радиовещательные станции, радиомикрофоны, радиостетоскопы, беспроводные видеокамеры
NFM	8...12 кГц	Системы персональной радиосвязи, радиомикрофоны, радиостетоскопы, беспроводные видеокамеры
SSB	3...5 кГц	Радиотелеметрия, телевидение
CW		Передача сигналов азбуки Морзе

Рекомендации по применению фильтра по частоте. Фильтр-классификатор по частоте позволяет пользователю оставить в базе данных обнаруженных сигналов для последующего анализа и идентификации только сигналы из заданных частотных диапазонов и убрать лишние сигналы.

В настоящее время разработчики СТС в качестве задающих генераторов радиомикрофонов наиболее широко применяют резонаторы на базе поверхностно-акустических волн (ПАВ). Рабочие частоты данных резонаторов, а следовательно, и СТС на их основе, могут быть сгруппированы в фиксированное количество наиболее опасных частотных диапазонов. Ниже указаны типовые частотные диапазоны данных резонаторов:

292...294 МГц; 302...326 МГц; 378...391 МГц; 402...434 МГц;

857...868 МГц; 914...916 МГц; 979...981 МГц.

Необходимо понимать, что указанные частотные диапазоны не перекрывают всех возможных частот работы СТС, но являются приоритетными для анализа при поиске наиболее распространенных СТС со стандартными видами модуляции сигналов.

Рекомендации по применению фильтра по полосе частот. Ширина спектра большинства СТС со стандартными видами модуляции является прогнозируемым значением. В табл. 5.1 приведены стандартные значения ширины спектра для различных модуляций и возможные легальные и нелегальные источники таких сигналов.

Применение фильтра-классификатора по полосе частот позволяет отобрать для анализа из всех обнаруженных сигналов только те, которые удовлетворяют заданным требованиям по ширине спектра сигнала. Например, исключать из анализа узкополосные сигналы при необходимости анализа широкополосных сигналов.

ВАЖНО! Корректность измерения ширины спектра сигнала комплексом зависит от правильности выставления порогов обнаружения и различения. Разработчики рекомендуют устанавливать порог обнаружения на 15...25 дБ выше уровня естественного радиошума, а порог

различения рекомендуется устанавливать на 10...15 дБ ниже порога обнаружения.

Рекомендации по применению фильтра превышения порога. Применение фильтра-классификатора по превышению порога позволяет отобрать из всего многообразия обнаруженных сигналов только те, которые удовлетворяют заданным требованиям по уровню сигнала. Фильтр-классификатор оставит в базе данных сигналы, уровень которых больше порога различения на заданную величину. Применение данного фильтра основано на предположении, что сигнал СТС находящегося в ближней зоне антенной системы комплекса имеет заведомо высокую амплитуду.

Использование фильтра целесообразно при анализе базы данных обнаруженных сигналов, полученной после предварительного сканировании диапазона с низким предустановленным порогом обнаружения (например, при поиске шумоподобных сигналов). После сканирования шумоподобные сигналы выделяются для анализа при помощи фильтра по полосе частот, а остальные сигналы — при использовании фильтра превышения порога. При этом естественный радиошум, неизбежно попадающий в базу данных при сканировании с низким порогом обнаружения, не мешает анализу.

Для корректного использования фильтра-классификатора рекомендуется учитывать, что амплитуда принятого сигнала, а следовательно, и величина превышения порога, зависит от следующих факторов:

- выходной мощности передатчика СТС (чем выше выходная мощность, тем выше амплитуда принятого сигнала);
- ширины полосы передатчика СТС. При одинаковой выходной мощности амплитуда сигнала СТС с более узкой полосой (например, NFM) будет больше амплитуды сигнала с более широкой полосой (например, WFM);
- расположения приемной антенны комплекса относительно антенные передатчика СТС в пространстве.

Рекомендуемое значение порога превышения для устройств негласного контроля информации с сосредоточенным спектром (WFM, NFM, AM) и выходной мощностью от 10 мВт составляет + 15 дБ (указанное значение рекомендуется для устанавливаемых порогов).

При работе с комплексом необходимо учитывать, что внутренняя антенная система комплекса, как правило, регистрирует не прямой сигнал от устройства негласного контроля информации, а переотраженный. Это обстоятельство необходимо учитывать при установке превышения в децибеллах, так как может возникнуть такая ситуация, когда внутренняя антенна будет находиться в точке замирания сигнала. Чтобы исключить влияние данного явления на качество прове-

дения радиомониторинга, рекомендуется размещать внутреннюю антенную систему комплекса в разных местах обследуемого помещения. Это приведет к усреднению амплитуд принятых сигналов.

Рекомендации по применению фильтра по регулярности. При проведении поисковых мероприятий подключение данного фильтра-классификатора позволяет проводить раздельный анализ сигналов постоянно действующих передатчиков и сигналов радиосредств, периодически выходящих в эфир. Поскольку большинство передатчиков СТС работают в непрерывном режиме, использование данного фильтра позволяет исключить из числа анализируемых краткосрочные сигналы «легальных» передатчиков, в том числе с модуляциями, сходными с модуляциями передатчиков СТС, — сигналы от радиостанций, «служебных» каналов управления и т. п.

Некоторые типы СТС могут оснащаться системой активации голосом (VOX/VOR). Для принудительного перевода таких СТС в режим непрерывной передачи рекомендуется при проведении поисковых мероприятий использовать подзвучку, например музыку CD проигрывателя.

Сигналы некоторых СТС могут находиться в эфире не постоянно (СТС с дистанционным управлением, СТС с накоплением, СТС с псевдослучайной перестройкой рабочей частоты (ППРЧ)). Для распознавания таких сигналов необходимо использовать специальные алгоритмы, которые будет рассмотрены ниже. Однако выделение таких сигналов для анализа из общей базы данных может эффективно производится с помощью фильтра по регулярности. Рекомендуемое значение по регулярности для непрерывных сигналов от 85 % до 100 %.

Рекомендации по применению фильтра по числу обнаружений. Применение фильтра-классификатора по числу обнаружений позволяет оставить в базе данных только те сигналы, число обнаружений которых больше заданного. Подключение данного фильтра-классификатора позволит удалить из списка обнаруженных однократные или кратковременные сигналы. Использование этого фильтра целесообразно совместно с фильтром по отношению уровней.

Рекомендации по применению фильтра по отношению уровней. Количество обнаруженных сигналов и их спектральных компонентов, с которыми оперируют современные широкодиапазонные системы радиоконтроля с учетом их высокой чувствительности и частотного разрешения, может достигать в условиях крупного города нескольких сотен и даже тысяч. Программные средства классификации компьютерных комплексов радиоконтроля на основе анализа определенных признаков, например значений несущих частот, уровней, ширины и формы спектра, времени и регулярности появления, отбирают из всего множества обнаруженных сигналов только те, которые представляют

действительный интерес для оператора или подсистемы регистрации. Такой подход значительно повышает эффективность и скорость анализа собранной комплексом радиоконтроля информации, сокращая количество интересующих сигналов в десятки и сотни раз.

Среди фильтров-классификаторов различных видов необходимо выделить пространственный фильтр по отношению уровней, задача которого состоит в том, чтобы разделить все обнаруженные сигналы на две группы: излучаемые внешними источниками, расположенными на значительном удалении от контролируемой зоны, и локальные, создаваемые внутри таких зон. Принцип работы данного фильтра-классификатора основан на простых физических соображениях: внешний источник излучения находится на значительном удалении от разнесенных антенн, поэтому мощность создаваемого им сигнала в каждой антенне будет примерно одинаковой. С другой стороны, локальный источник оказывается в непосредственной близости от одной из антенн и поэтому наводит в ней существенно больший уровень, чем в других удаленных от него антеннах.

Для реализации пространственного метода классификации комплекс радиоконтроля необходимо оснастить несколькими пространственно разнесенными антеннами, которые обычно подключаются к радиоприемнику через антенный коммутатор. Фильтр-классификатор по отношению уровней может существенно ускорить выявление нелегальных радиопередатчиков и других источников утечки информации по радиоканалу из внутренних помещений зданий даже в условиях сильной загрузки радиодиапазона внешними станциями. Несомненное достоинство классификатора такого типа состоит в том, что он использует только один демаскирующий признак сигнала — уровень излучаемой мощности и не требует анализа его информационных, спектральных и иных характеристик.

Применение фильтра-классификатора по отношению уровней позволяет оставить в базе данных только те сигналы, отношение уровней которых больше заданного оператором.

Применение данного фильтра-классификатора позволяет реализовать процедуру идентификации излучений методом разнесённого приёма. При применении метода разнесённого приёма делаются следующие предположения:

а) «внешние» сигналы от легальных источников (радио- и телевизионные ретрансляторы, базовые станции сетей сотовой связи и т. д.) будут наводить примерно одинаковую ЭДС (амплитуду сигнала) в опорной (внешней) и внутренней антеннах (в проверяемом помещении). Это предположение основано на том, что, как правило, такие сигналы обладают высокой мощностью и не испытывают существен-

ного ослабления, распространяясь сквозь ограждающие конструкции здания;

б) «внутренние» сигналы от устройств негласного контроля информации будут наводить существенно отличные ЭДС в опорной и внутренней антеннах. В свою очередь, это предположение основано на том, что сигналы от устройств негласного съема информации обладают низкой мощностью (десятки мВт). Это обстоятельство приводит к тому, что такой сигнал будет наводить высокое ЭДС во внутренней антенне (в так называемой ближней зоне) в виду малого расстояния до устройства негласного съема информации. Вместе с тем такой сигнал будет испытывать существенное ослабление, распространяясь сквозь ограждающие конструкции здания, и, как следствие, наведет малое ЭДС в опорной (внешней) антенне.

Для получения максимального эффекта от использования метода разнесённых антенн рекомендуется обеспечить максимальную базу (расстояние) между антеннами.

Применять данный фильтр-классификатор рекомендуется совместно с фильтром по числу обнаружений, чтобы исключить из обработки случайные однократные сигналы.

Предполагаемое отношение уровней A, дБ, используемое для настройки данного фильтра, вычисляется с помощью следующего выражения:

$$A = 20 \lg(r_2/r_1),$$

где r_1 — расстояние от внутренней антенны до предполагаемого места установки устройства негласного контроля информации; r_2 — расстояние от внешней антенны до предполагаемого места установки устройства негласного контроля информации.

Пример. Пусть $r_1 = 3$ м, а $r_2 = 30$ м. Тогда ожидаемое отношение уровней $A = 20 \lg(30/3) = 20$ дБ. Но ввиду того, что, как правило, внутренняя антенна комплекса регистрирует не прямой сигнал от источника, а переотраженный, рекомендуемое отношение уровней сигналов должно быть на 6...8 дБ меньше ожидаемого.

Рекомендуемая последовательность применения фильтра по отношению уровней:

1. В закладке «Устройства» меню «Настройки» установить потери для 30-метрового кабеля 5 дБ. Указанная величина для кабелей большей длины должна подбираться экспериментально.

2. Запустить комплекс на сканирование в заданном диапазоне частот. Число циклов сканирования должно быть не менее 30.

3. Кнопкой «Стоп» остановить сканирование.

4. В закладке «Фильтры» меню «Настройки» подключить фильтр по числу обнаружений. Рекомендуемое значение для данного фильтра не менее 20.

5. В закладке «Фильтры» меню «Настройки» подключить фильтр по отношению уровней. Рекомендуемое значение для данного фильтра рассчитывается по вышеописанной формуле.

Рекомендации по применению фильтра по совпадению спектра. Применение фильтра-классификатора по совпадению спектра позволяет оставить в базе данных только те сигналы, совпадение спектра которых с эталоном больше заданной оператором величины. Под эталоном понимаются спектры сигналов некоторых устройств негласного контроля информации, причем, чем больше будет накоплено эталонов, тем более корректно будет проведена процедура сравнения. Метод корреляции, используемый в комплексе, предназначен для выявления радиомикрофонов. Метод корреляции основан на сравнении огибающей радиосигнала с эталоном, сохраненным в базе данных.

Рекомендации по применению режимов экспресс-анализа векторного анализатора сигналов. Комплекс позволяет анализировать тонкую структуру сигналов с помощью шести режимов экспресс-анализатора. Возможно представление сигнала в частотной области (режим «Спектр»), во временной области (режим «Амплитуда»), в трехмерном представлении — время, частота и уровень (режим «Спектрограмма»). Кроме того, векторный анализатор комплекса позволяет анализировать модулирующие функции сигналов, а именно зависимость частоты и фазы сигнала от времени (режимы «Частота» и «Фаза» соответственно). Особенностью данного комплекса является возможность векторного анализа сигнала (режим «Вектор»).

Рекомендации по применению режима амплитуда. Выбор данного режима экспресс-анализа позволяет анализировать структуру сигнала во временной области. По сути данный режим позволяет работать с комплексом как с обычным осциллографом (за исключением возможности синхронизации «картинки»). Применение режима «Амплитуда» удобно на этапе идентификации обнаруженного сигнала.

Например, при идентификации сигналов от скрытых видеокамер с передачей информации по радиоканалу. При анализе таких излучений в режиме «Амплитуда» должна наблюдаться характерная для стандартных телевизионных сигналов с АМ модуляцией структура (строчные синхроимпульсы, кадровые синхроимпульсы, сигналы изображения). На рис. 5.1 представлена типовая осциллограмма телевизионного сигнала от скрытой видеокамеры с передачей информации по радиоканалу. Кроме того, обнаружение сигнала с такой структурой на частотах вне диапазона телевизионного вещания практически однозначно свидетельствует о работе передатчика скрытой видеокамеры.

Рекомендации по применению режима «Спектрограмма». Выбор данного режима экспресс-анализа позволяет отображать изменение спектральной панорамы во времени. При этом по оси абсцисс

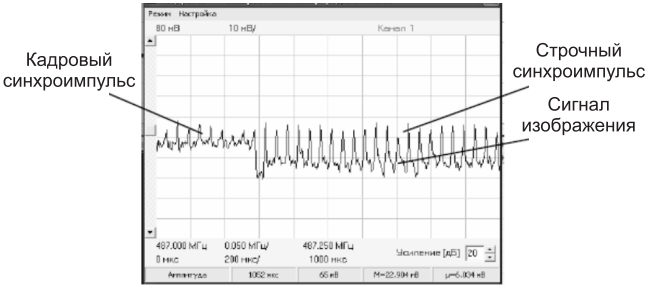


Рис. 5.1. Осцилограмма телевизионного сигнала

(горизонтальная линия) будет отложена частота, а по оси ординат (вертикальная линия) время. Цветовой кодировкой будёт передаваться уровень сигнала (фиолетовый цвет — слабые сигналы, красный цвет — сильные).

Применение режима «Спектрограмма» является единственной возможностью обнаружить и идентифицировать сигналы от устройств негласного контроля информации с псевдослучайной перестройкой рабочей частоты (ППРЧ). Аппаратно комплекс позволяет анализировать сигналы в полосе до 50 МГц и сигналы кратковременных передач [до 1,5 секунд при полосе обзора 120 МГц].

В окне спектрограммы сигналы от устройств негласного контроля информации с ППРЧ, как правило, отображаются в виде кривых с определённой периодичностью и характерным рисунком. Например, на рис. 5.2 представлен сигнал от закладного устройства с линейно изменяющимся законом частоты.

Кроме того, применение режима «Спектрограмма» может быть полезным на этапе идентификации излучений от несанкционированно включенных в помещении радиотелефонов (в том числе переделанных под СТС).

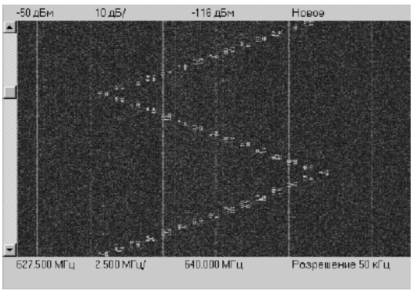


Рис. 5.2. Спектрограмма сигнала от ЗУ с ППРЧ

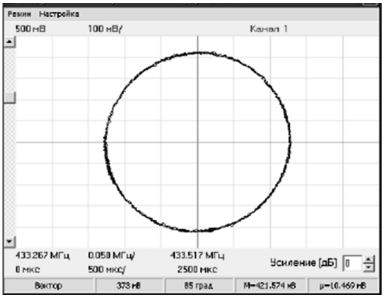
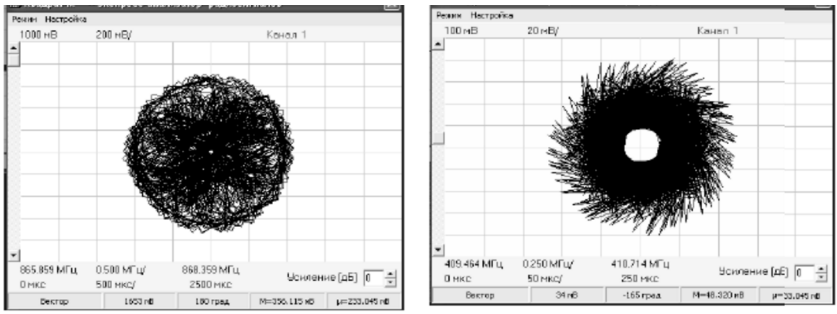


Рис. 5.3. Векторная диаграмма сигнала с частотной модуляцией



а) *б)*

Рис. 5.4. Устройства с амплитудно-импульсной манипуляцией (*а*) и дельта-модуляцией (*б*)

Рекомендации по применению режима «Вектор». Выбор данного режима экспресс-анализа позволяет отображать комплексную огибающую радиосигнала. Векторная диаграмма при этом отображает траекторию конца вектора с началом в центре координат, модуль которого равен амплитуде сигнала, а угол с горизонтальной осью — фазе. Анализ траектории комплексного вектора при изменении времени позволяет распознать вид модуляции. Например, сигнал с постоянной амплитудой и частотной модуляцией выглядит в виде окружности с центром в начале координат (рис. 5.3).

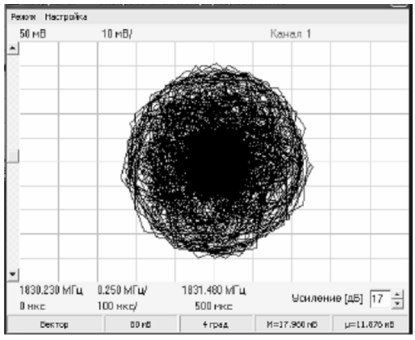


Рис. 5.5. Векторная диаграмма сигнала цифрового канала системы GSM-1800

Применение данного режима рекомендуется при анализе сигналов с многопозиционной фазовой и амплитудно-фазовой манипуляцией. В зависимости от передаваемого символа фазы и амплитуды таких сигналов попадают на определённые точки комплексной плоскости. Данный режим удобен на этапе идентификации сигналов от несанкционированно включенных сотовых телефонов, устройств негласного контроля информации с цифровыми видами модуляции. Например, на рис. 5.4 представлены векторные диаграммы от закладочных устройств с амплитудно-импульсной манипуляцией и дельта-модуляцией. Для сравнения на рис. 5.5 приведена векторная диаграмма сигнала цифрового канала системы GSM-1800.

Рекомендации по применению режимов усреднения. Режим усреднения позволяет выделять слабые сигналы на уровне шумов. Дан-

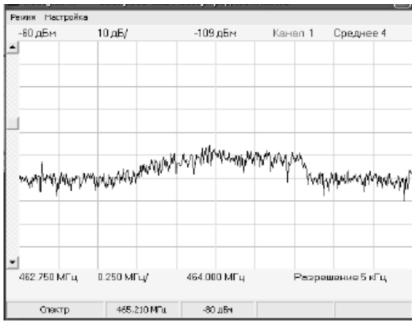


Рис. 5.6. Спектр широкополосного сигнала с 4-кратным усреднением

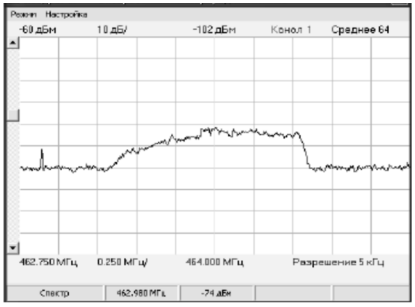


Рис. 5.7. Спектр широкополосного сигнала с 64-кратным усреднением

ный режим рекомендуется использовать, если есть априорная информация о возможности установки устройства негласного контроля информации с использованием широкополосных шумоподобных сигналов. Спектр таких сигналов распределен по широкой полосе частот, в результате чего уровни гармоник сигнала имеют крайне малую амплитуду, соизмеримую с естественными шумами. Как следствие, такие сигналы обладают высокой скрытностью.

Комплекс с помощью режима усреднения позволяет уверенно обнаруживать такие сигналы. Например, на рис. 5.6 и 5.7 представлены спектры широкополосных сигналов с 4- и 64-кратным усреднением.

Рекомендации по применению режимов накопления максимумов. Режим накопления максимумов позволяет накапливать максимальные значения за все время анализа спектра в заданной полосе частот. При этом текущее значение уровня спектра в каждой частотной точке заменяет предыдущее только в том в случае, когда оно больше предыдущего. Применение данного режима рекомендуется для обнаружения слабых краткосрочных (импульсных) сигналов.

Рекомендации по применению режима регистрации для поиска закладных устройств с ДУ. Комплекс позволяет обнаруживать и регистрировать сигналы от устройств негласного контроля информации с пультом дистанционного управления (ДУ). Для регистрации сигналов от таких устройств необходимо накопить базу данных обнаруженных сигналов в заданном диапазоне частот. Затем выполнить следующие операции:

1. В закладке «Панорама» панели «Настройка» необходимо выбрать из выпадающего списка (от 1 до 100) число циклов обзора, после которых программа будет автоматически выполнять обработку базы данных обнаруженных сигналов и выполнять запрос к базе данных.

2. В меню «Режим» командой «Регистрация» необходимо установить режим автоматической регистрации. После выбора данного

режима программа выведет сообщение: «Включить фильтр сигналов по дате/времени?». Если согласиться с включением этого фильтра, то в список обнаруженных сигналов будут заноситься только «новые» сигналы, время обнаружения которых больше времени начала текущего цикла.

3. Для автоматической регистрации звукового сигнала на жесткий диск компьютера необходимо установить «Параметры регистрации» в закладке «Регистрация» панели «Настройки».

После выполнения описанных установок и нажатия на кнопку «Старт» программа выполнит заданное количество циклов сканирования, обработает данные радионаблюдения и откроет окно анализатора спектра. В этом окне будут последовательно отображаться спектры всех вновь обнаруженных сигналов (в том числе сигнал от включенного по ДУ закладного устройства). Программа запишет фонограмму каждого «нового» сигнала в звуковой файл.

Особенность программы в том, что перед записью фонограммы она анализирует наличие сигнала на частоте. Если сигнал к моменту записи фонограммы пропал, программа переходит к следующему в списке сигналу, выполняет его анализ и регистрацию.

Рекомендации по поиску радиомикрофонов с системой VOX. Активизация радиомикрофонов, оснащенных системой VOX, осуществляется с помощью фонового акустического сигнала. В качестве акустического фона рекомендуется использовать речевую фонограмму с магнитофона или звуковой сигнал с радиоприемника, размещенных в контролируемом помещении. Выбор громкости тестового звукового сигнала определяется как размерами помещения, так и чувствительностью микрофона закладочного устройства. Обычно микрофоны закладочных устройств уверенно воспринимают звук средней громкости с расстояния порядка 10 м.

Рекомендации по обнаружению новых сигналов. Комплекс позволяет обнаруживать новые сигналы. Данная процедура удобна при эксплуатации комплекса в выделенном помещении не постоянно, а с определенной периодичностью (например, через неделю). При этом обнаружить новые сигналы в базе данных можно следующим образом:

1. Загрузить старую базу обнаруженных сигналов.

2. Запустить комплекс на сканирование в заданном диапазоне частот.

3. Остановить процесс сканирования.

4. В базе данных обнаруженных сигналов в столбце «Дата/Время» среди всех сигналов найти сигналы с текущим временем обнаружения. Процедура поиска новых сигналов в столбце «Дата/Время» упрощается, если кликнуть по его заглавию. При этом сигналы в базе

данных должны выстроиться в порядке убывания их времени обнаружения.

Полученная в ходе предварительного радиомониторинга информация, как уже было указано, должна быть проанализирована с целью определения принадлежности обнаруженных сигналов неизвестного назначения к тому или иному виду ЗУ.

Основным способом распознавания сигналов является идентификация вида модуляции типа сигнала, который используется в сигнале передатчика, с помощью слухового контроля или инструментов технического анализа и сопоставление полученных данных сданными о вероятных видах сигналов, которые могут использоваться в несанкционированных радиопередающих устройствах.

Для передачи сигнала применяются аналоговые и цифровые виды модуляции.

Модуляция сигнала применяется для обеспечения возможности передать с помощью неинформационного высокочастотного сигнала низкочастотное информативное сообщение. При модуляции какой-либо из трех основных параметров высокочастотного сигнала меняется по закону, который задается информативным низкочастотным сигналом.

Если изменения параметра сигнала происходят непрерывно, то модуляция считается аналоговой, если дискретно, то цифровой. Аналоговые виды модуляции применяются в ЗУ для передачи аналоговых информационных сигналов — звука или видео, собственные парметры которых меняются также непрерывно. Цифровые виды модуляций применяются для передачи цифровых сигналов, которые сами принимают дискретные значения.

Основными видами аналоговой модуляции являются: амплитудная модуляция, частотная модуляция и фазовая модуляция. Наиболее часто в закладочных устройствах применяется частотная модуляция.

Частота несущей (модулируемого колебания) непрерывно меняется в зависимости от частоты модулирующей функции.

В основе цифровых видов модуляций лежит дискретное изменение параметра модулируемого сигнала.

Из цифровых видов модуляций наиболее часто применяются в ЗУ сигналы с ASK, FSK, PSK модуляциями:

ASK — вид модуляции, при котором дискретно меняется амплитуда сигнала;

FSK — вид модуляции, при котором дискретно меняется частота сигнала;

PSK — вид модуляции, при котором дискретно меняется фаза сигнала.

Изменяющиеся параметры могут принимать минимум два (0 и 1) или более (4, 6, 8 и т. д.) значений. Например, дискретные фазовые модуляции называются по количеству значений, принимаемых фазой: BPSK — для двух значений, QPSK — для четырех значений и т. д.

Не всегда при передаче сигнал присутствует в эфире непрерывно. Рассмотрим случаи, когда сигнал может быть нестационарен во времени.

ППРЧ-сигналом называется сигнал, который перестраивается по дискретным частотным значениям в ограниченной полосе частот. Такие нестационарные сигналы применяются в системах связи для повышения помехоустойчивости канала связи, для экономии питания и для увеличения ёмкости канала. В ЗУ, кроме указанных выше целей, такие сигналы применяются для повышения скрытности. Как правило, перестройка осуществляется по псевдослучайному закону и частоты настройки повторяются только через довольно большой промежуток времени. Примером использования ППРЧ в системах связи является, например, Bluetooth.

TDMA — временно́е разделение доступа. Современные каналы связи перегружены, и возникает необходимость использования одного частотного канала несколькими передатчиками. С другой стороны, современные алгоритмы сжатия позволяют передавать сигнал значительно быстрее во времени, чем он записывался. На основе этого разработана технология TDMA: каждый передатчик выходит в эфир четко в установленный для него интервал времени (тайм-слот). Тайм-слот одного передатчика повторяется периодически. В то время пока передатчик неизлучает и ждет свой тайм-слот, он записывает и сжимает информацию. Таким образом, на одной частоте, не мешая друг другу, могут работать несколько передатчиков. Примерами сигналов с временны́м разделением доступа являются, например, сигналы GSM и DECT. В GSM это не так очевидно, из-за высокой загруженности канала. В DECT можно наблюдать, как из-за того, что не все тайм-слоты заняты передатчиками, сигнал DECT на одной частоте появляется и исчезает во времени.

В ЗУ этот принцип используется также для повышения скрытности передачи (ЗУ с накоплением). Информация копится в ЗУ в течение достаточно длительного промежутка времени (при этом ЗУ ничего не излучает и, следовательно, не может быть обнаружено средствами радиомониторинга), а затем передается в эфир в течение короткого интервала времени. В современных ЗУ коэффициент сжатия может доходить до 60. Это значит, что 8 часов записанной звуковой информации могут быть переданы за 8 минут.

Другим способом повышения качества функционирования каналов радиосвязи является расширение спектра сигнала. Существуют

несколько видов расширения спектра. Основными задачами расширения спектра является увеличение помехозащищенности каналов передачи информации и расширение пропускной способности канала. В ЗУ, кроме указанных выше задач, расширение спектра используется для повышения скрытности передаваемого сигнала ЗУ, поскольку если широкополосный сигнал принимается приемником, полоса анализа которого меньше полосы сигнала, такой сигнал будет выглядеть как шум с высоким уровнем.

DSSS, или прямое расширение спектра. Сущность метода состоит во введении в исходный цифровой сигнал дополнительных кодов, которые из-за своей избыточности позволяют восстановить на приемном конце исходный сигнал без ошибок, даже если при передаче в сообщении есть ошибки. Введение дополнительного кода увеличивает объем передаваемой информации и соответственно расширяет спектр сигнала, который необходим для его передачи. Прямое расширение спектра используется, например, в сигналах CDMA.

OFDM — это способ увеличения пропускной способности канала, когда в одном канале передается несколько поднесущих частот с информационным сигналом. Современные методы обработки сигналов позволяют разделить поднесущие на приемной стороне без потерь качества за счет использования цифровых фильтров. Это возможно только при использовании специальных приемников, которые рассчитаны на работу с такими сигналами. В остальных случаях на частотном спектре такой сигнал выглядит как единый широкополосный сигнал, поскольку эти несущие расположены на соседних частотах, но так близко друг от друга, что спектры поднесущих пересекаются. OFDM сигналы используются, в частности, в Wi-Fi технологии.

Простейшим инструментом распознавания вида модуляции является слуховой контроль демодулированного сигнала. Если используется аналоговый вид модуляции и приемник имеет соответствующий демодулятор, то оператор может прослушать информацию и принять решение об опасности сигнала. Однако в современных ЗУ для скрытия сигнала от средств наблюдения может применяться инверсия спектра низкочастотного сигнала. При этом спектр исходного низкочастотного сигнала, как правило аналогового, инвертируется (переворачивается). За счет инверсии разборчивость сигнала даже после корректной демодуляции оказывается низкой и повышается вероятность признания сигнала ЗУ неинформативным.

Итак, преобразованный в цифровую форму сигнал может быть представлен по разному. Возможность анализа сигнала в нескольких представлениях позволяет распознать виды модуляции, которые в одном представлении абсолютно неразличимы, а в другом имеют характерные признаки и могут быть по ним идентифицированы.

Исходно сигнал поступает с цифрового приемного устройства в виде дискретных отсчетов. Если эти отсчеты расположить в системе координат время/амплитуда, то сигнал можно представить в виде осциллограммы. Представление в виде осциллограммы удобно для идентификации сигналов, например, с ASK модуляцией, когда дискретное изменение амплитуды сигнала может быть различимо на осциллограмме.

Осциллограмму можно построить как для высокочастотного сигнала, так и для исходного демодулированного сигнала. В этом случае на осциллограмме можно будет различать импульсы, соответствующие исходной цифровой информации, которая передавалась сигналом.

С помощью алгоритма БПФ временные отсчеты позволяют представить сигнал в виде частотного спектра в координатах амплитуда–частота. Представление в виде спектра позволяет распознавать многие виды модуляции по характерным спектральным образам.

Еще одно представление сигнала — векторное. В этом представлении сигнал представляется в круговой системе координат в виде вращающегося вектора, такую систему координат называют фазовой плоскостью. При этом длина вектора соответствует амплитуде сигнала, а угол поворота — фазе сигнала. Очевидно, что такое представление позволит индентифицировать сигналы, которые используют дискретную фазовую модуляцию, поскольку каждому значению фазы будет соответствовать точка на фазовой плоскости. Векторная диаграмма может быть представлена либо в виде линий, соединяющих точки на плоскости, либо в виде самих точек.

И, наконец, сигнал можно представить в виде временного спектра-«водопада». Такое представление сигнала псевдотрехмерно, по осям координат откладываются время и частота сигнала, а цветом отображается уровень сигнала в данной точке. Такое представление сигнала удобно для анализа нестационарных и быстро меняющихся во времени сигналов, например сигналов ППРЧ или TDMA.

Таким образом, использование такого многообразия средств и способов преобразования «опасных» сигналов, передаваемых ЗУ, требует от оператора определенных знаний и навыков в их обнаружении и распознавании. Поэтому для выявления ЗУ, кроме идентификации вида модуляции и типа сигнала, используются основные демаскирующие признаки радиосигналов. Основными разведпризнаками, которые могут демаскировать сигналы ЗУ, являются:

- уровень сигнала (энергетический признак);
- частота сигнала (частотный признак);
- время появления сигнала (временной признак).

Вторичными разведпризнаками могут являться:

- форма спектра, осциллограммы или векторной диаграммы сигнала (спектральный признак);
- информативная составляющая сообщения, которое предается сигналом (информационный признак).

Вторичными эти признаки являются главным образом потому, что в реальных условиях получить их и проанализировать зачастую оказывается технически сложно или невозможно.

Кроме того, можно выделить параметры сигналов, которые могут дополнять определенные выше разведпризнаки. Например, полоса сигнала может дополнять частоту сигнала в частотном признаке.

Рассмотрим динамику определения активных радиоизлучающих ЗУ по демаскирующим признакам.

Энергетический признак. Обнаружение сигнала по энергетическому признаку основано на превышении уровнем сигнала установленного оператором порога. В этом случае разведпризнаком сигнала является уровень сигнала.

Порог — это задаваемое вручную или автоматически условное значение. Если уровень излучения на данной частоте превышает это значение, то излучение считается сигналом, а если не превышает — шумом. Поскольку порог это условное значение, то любой сигнал можно считать частным случаем шума.

Под уровнем сигнала в программе понимается либо усредненная за некоторый промежуток времени (время измерений) спектральная плотность мощности, либо усредненная амплитуда сигнала на данной частоте.

Спектральная плотность мощности сигнала — это мощность сигнала, приведенная, в общем случае, к 1 Гц. Для спектров, построенных с помощью дискретных алгоритмов (например БПФ), под спектральной плотностью мощности понимается мощность, приведенная к одной спектральной составляющей спектра.

Амплитуда сигнала — это мгновенное значение напряжения сигнала на данной частоте.

Основное отличие спектральной плотности мощности и амплитуды сигнала от мощности состоит в том, что спектральная плотность и амплитуда сигнала не зависят от полосы измерения и указываются для конкретной частоты, а мощность зависит от полосы и неудобна для использования в качестве параметра сигнала на конкретной частоте.

Отличие спектральной мощности от амплитуды сигнала состоит в том, что амплитуда — это оценка напряжения сигнала на частоте, а спектральная мощность — это оценка мощности на частоте.

Спектр сигнала в программе — это кривая значений спектральной плотности мощности или амплитуды сигнала и шума в полосе.

Мощность сигнала — это площадь под спектром сигнала в полосе сигнала.

Полоса сигнала — это оценка ширины спектра сигнала.

Соотношение сигнал/шум — это отношение мощности сигнала к мощности шума. Оно зависит от полосы измерения, поскольку для сигнала мощность не изменяется от полосы измерений, пока полоса измерения больше полосы сигнала (подразумевается, что в случае корректных измерений это так), а для шума мощность зависит от полосы измерений, поскольку полоса шума считается бесконечной, следовательно, любая полоса измерений всегда меньше полосы шума.

Чем уже полоса измерения, тем меньше мощность шума и соответственно выше соотношение сигнал/шум. Таким образом, если на «Панораме» сигнал находится слишком близко к шуму и нельзя его рассмотреть, то можно открыть этот сигнал в «Анализаторе» в более узкой полосе (но не менее полосы сигнала) и проанализировать сигнал с достаточным соотношением сигнал/шум.

Уровень сигнала отображается в программе в окне «Список» на соответствующих маркерах, а в числовом и в графическом (в виде спектра) видах — в окнах «Панорама» и «Анализатор/Спектр» на радиочастотном спектре.

Частотный признак. Использование частотного разведпризнака основано на оценке местоположения частоты сигнала в радиочастотном спектре относительно мест возможного расположения легальных или нелегальных сигналов.

Частота сигнала — это скорость измерения фазы сигнала. Для определения и измерения частоты сигнала в программе используется метод оценки усредненного значения частоты максимальной спектральной составляющей сигнала.

Для получения спектра сигнала, в котором можно оценить спектральные составляющие, исходный сигнал преобразуется в частотный спектр с помощью алгоритма БПФ. Этот алгоритм позволяет преобразовать исходный сигнал из системы координат амплитуда–время в систему координат частота–амплитуда. Окна программы «Панорама» и «Анализатор/Спектр» представляют сигнал именно в виде спектра.

Дополнительным параметром при обнаружении несанкционированного сигнала по частотному разведывательному признаку является полоса сигнала. Использование частоты и полосы сигнала как одного демаскирующего признака позволяет повысить достоверность частотного разведпризнака.

Существуют два основных метода измерения полосы сигнала.

Ширина полосы сигнала определяется как ширина полосы частот, за верхней и нижней пределами которой излучаемые средние мощнос-

ти равняются определенному проценту K от всей средней мощности данного излучения. Нормативные документы регламентируют принимать значение R равным 1 % для большинства классов излучений.

Ширина полосы частот сигнала определяется как часть излучения сигнала, за пределами которой любая дискретная составляющая спектра внеполосных радиоизлучений ослаблена относительно заданного уровня не менее чем до уровня X дБ. Обычно в качестве заданного уровня используется 0 дБ, а X приравнивается 30 дБ.

Поскольку определение нулевого уровня для большинства цифровых сигналов затруднительно, в программе используется первый метод измерения ширины полосы сигнала.

Временной признак. Обнаружение радиосигнала по временному признаку основано на сопоставлении времени появления сигнала (превышение уровнем излучения порога на частоте сигнала) и времени отсутствия сигнала в эфире с возможными временными промежутками работы несанкционированных передатчиков или с известными особенностями поведения во времени некоторых типов сигналов.

Время появления сигнала — это момент времени, в который уровень сигнала превысил порог.

Существуют несколько параметров сигналов, которые прямо или косвенно имеют отношение к временному разведпризнаку:

- время первого обнаружения сигнала;
- время начала и окончания каждого сеанса сигнала;
- признак активного и неактивного (обнаруженного ранее, но не обнаруживаемого впоследствии в течении заданного интервала времени сигнала);
- «водопад» — представление сигнала в координатах время/частота/уровень, которое позволяет совместить обнаружение сигнала по частотному и временному признакам и по выявленным особенностям поведения сигнала во времени отнести сигнал к некоторым известным типам сигналов.

Полученная в ходе предварительного радиомониторинга и анализа обнаруженных сигналов информация позволяет наиболее полно определиться как со временем, необходимым на проведение проверки, так и со спецефическим оборудованием, необходимым для её качественного проведения.

Завершение подготовительного этапа. Работы подготовительного этапа обычно завершаются разработкой документов, подтверждающих легенду прикрытия при проведении различных видов поисковых и исследовательских работ, а также специальных бланков и заготовок документов, ускоряющих регистрацию промежуточных результатов запланированных работ.

Для сокращения непроизводительных затрат времени в ходе непосредственного проведения специальной проверки помещений целесообразно заранее подготовить:

- схемы коммуникаций и планы проверяемых помещений, на которые будут наноситься отметки мест обнаружения средств НСИ и подозрительных мест;
- бланки протоколов будущих измерений;
- журналы регистрации заводских и инвентарных номеров проверенного оборудования;
- журналы регистрации мест установки пломб и скрытых меток, способствующих ускорению работ при последующих специальных проверках;
- карту занятости радиоэфира;
- базу данных выявленных и идентифицированных радиосигналов;
- список частот «подозрительных» радиоизлучений.

Следует помнить, что в отличие от документов, подтверждающих легенды прикрытия, все документы, подготавливаемые для работ по непосредственному проведению проверки, относятся к категории конфиденциальных и не подлежат разглашению среди сотрудников предприятия.

Перед началом непосредственного проведения поисковых работ рекомендуется осмотреть прилегающие к предприятию улицы и близлежащую территорию для обнаружения возможно развёрнутых противником постов радиоконтроля. Подозрения должны вызывать автомобили, длительно находящиеся с людьми на одном месте. Рекомендуется записать номера вызвавших подозрение автомобилей, приметы находящихся в них людей и других подозрительных лиц. В случае обнаружения в помещениях ЗУ эти сведения могут пригодиться для установления конкретных лиц и организаций, причастных к негласному съёму защищаемой информации.

Визуальный осмотр помещения. Перед осмотром необходимо обратить внимание на возможные метки, которые могут оставляться с той или иной целью, в том числе и с целью фиксирования места размещения предметов, имеющих устройства съема информации. В качестве меток может быть использовано определенное расположение разных предметов, расположение на предметах в определенном порядке ниток, волосинок, следов пальцев, пыли и другие характерные пометки, а также метки, наносимые специальным химическим составом.

Осмотр и проверка предметов должны начинаться с визуального фиксирования или фотографирования мест расположения всех предметов в обследуемом пространстве. Работа начинается с подготовки контролируемого помещения (объекта) и поискового оборудования.

В помещении создаются условия, при которых обеспечивается минимально возможный уровень фона электрического поля. Это достигается отключением потенциальных источников повышения фона:

- средств оргтехники;
- ПЭВМ, преобразователей и блоков питания;
- базовых станций беспроводных телефонов;
- люминесцентных осветительных ламп и других электронных устройств и электроприборов.

Визуальный осмотр и проверку предметов, находящихся в местах проведения комплексной проверки, необходимо проводить от общего к частному. Сначала осмотру подлежит вся территория обследования. Для этого один из опытных сотрудников — участников исследований медленно осматривает все предметы, обращая внимание на изменение расположения их от ранее установленного места (смещены, повернуты, переставлены местами друг относительно друга и т. д.) и на неплотно прилегающие к полу, стене или потолку предметы: палас, обои, ковры и т. д. Следует также обращать особое внимание на потемнение (осветление) обоев, ковров, пола, свежеокрашенные стены, потолки и другие изменившиеся особенности проверяемого помещения и находящихся в нем предметов интерьера.

После общего осмотра приступают к детальному осмотру конкретных предметов, который должен проводиться с учетом выявленных ранее особенностей. Осмотр всех предметов проводится со всех сторон.

При обследовании помещений мебель должна быть отодвинута от стен и друг от друга. Содержимое в столах, на столах, в шкафах и на полках должно быть переложено и визуально осмотрено.

При осмотре предметов быта и интерьера необходимо пристально осмотреть дверные ручки, запирающие устройства, вешалки, фирменные знаки и другие приспособления. Особое внимание следует обратить на подозрительные отверстия, инородные вставки, запачканные места и другие особенности предметов, находящихся на объекте поиска.

Осмотр необходимо проводить с помощью лупы, а недоступные места (межмебельные и вентиляционные проемы, места за батареями отопления, дымоходы и т. д.) осматривают с помощью досмотровых комплектов, представляющих собой портативные зеркала на раздвижной штанге, снабженные устройством подсветки, или с помощью эндоскопов, позволяющих осматривать труднодоступные места.

Целесообразно также закрыть окна и двери, опустить (задвинуть) шторы или жалюзи. Визуальный осмотр ограждающих конструкций, мебели и других элементов интерьера помещения на наличие в них ЗУ является обязательным и необходимым элементом поисковых работ.

Завершают осмотр детальным исследованием внешних поверхностей, полостей и внутренних поверхностей каждого предмета, элемента интерьера и конструкции помещения. В необходимых случаях используются фонари, досмотровые зеркала, лупы, эндоскопы.

При визуальном осмотре **пола** рекомендуется осмотреть снизу напольные покрытия (ковры, паласы, линолеум и т. п.), осмотреть поверхность пола. Исследовать места со следами недавней покраски, ремонта, применения инструмента, нарушающего целостность поверхности, проверить надежность крепления его элементов, осмотреть плинтусы. Тщательно исследовать места со следами недавнего ремонта и возможного вторжения, вскрыть и осмотреть подпольные каналы. Тщательно, на максимально возможную глубину с применением эндоскопа осмотреть содержимое труб, подходящих к подпольным каналам. Тщательно осмотреть места сквозного прохождения через пол водопроводных труб, труб парового отопления и других коммуникаций, поскольку в этих местах наиболее просто замаскировать следы вторжения при установке ЗУ.

Визуальный осмотр **стен** для сокращения времени осмотра целесообразно совмещать с осмотром развешенных на них предметов интерьера и покрытий. При осмотре стен необходимо освободить их поверхность от навешенных предметов и покрытий (картин, зеркал, ковров и т. п.), осмотреть поверхность стен, обращая особое внимание на места, отличающиеся по своей окраске или фактуре от остальной поверхности.

Обнаруженные подозрительные места отметить на плане помещения для последующего их исследования с помощью специальных технических средств.

При визуальном осмотре **вентиляционных** и других технологических отверстий и полостей рекомендуется снять закрывающую отверстие решётку, убедиться в отсутствии следов нарушения пылевого слоя вокруг отверстия и на внутренних его поверхностях, убедиться в отсутствии посторонних предметов и проводов в отверстии, полостях и подходящих к полости трубах, для чего использовать досмотровые зеркала, эндоскопы и фонари.

При визуальном осмотре **окон** необходимо провести осмотр поверхностей подоконника, оконного проёма и оконной рамы, обращая особое внимание на отсутствие посторонних проводников и предметов на внутренних и наружных поверхностях оконной рамы, следов демонтажа или замены уплотнений, запорных элементов, элементов крепления.

При визуальном осмотре **дверей** рекомендуется осмотреть щели за наличниками дверной коробки, убедиться в отсутствии следов демонтажа наличников, вскрытия дверной обивки и дверного полотна,

при осмотре металлической двери обратить особое внимание на следы высверливания отверстий в дверном полотне и дверной коробке.

При визуальном осмотре **потолка** следует обратить внимание на участки со следами недавней покраски, ремонта, протечек, сквозного прохождения труб и других коммуникаций. Особого внимания требует осмотр подвесного потолка. Осмотр подвесного потолка, как правило, совмещается с визуальным осмотром и проверкой линий и установленного на потолке оборудования проводных коммуникаций. Большие трудозатраты, связанные с визуальным осмотром подвесного потолка, требуют с особой тщательностью продумать технологию нанесения скрытых меток на устанавливаемые панели для облегчения последующего контроля их неприкосновенности. Виды меток, места и способы их нанесения обычно определяются на месте членом поисковой бригады и заносятся в виде схем, рисунков и пояснительного текста в специальный журнал регистрации пломб и скрытых меток.

Параллельно с осмотром ограждающих конструкций или по его завершении проводится визуальный **осмотр мебели** и других предметов интерьера. Осмотр мебели, как и помещения, обычно проводится от общего к частному: вначале осматриваются внешние поверхности основных конструктивных элементов, затем съёмных и внутренних элементов. Заканчивается осмотр исследованием пазов, отверстий и внутренних полостей.

Некоторые особенности имеет методика осмотра **встроенной мебели**. Обычно в виде встроенной конструкции выполняются платяной и книжный шкафы, стеллажи для документации, сейф. В ходе осмотра встроенной мебели особое внимание следует уделить исследованию декоративных покрытий и элементов конструкции, образующих заднюю стенку мебели, поскольку они могут скрывать полости, удобные для установки ЗУ. При осмотре такой мебели целесообразно прощупать и простучать наклеенные внутри обои, демонтировать внутренние декоративные покрытия и исследовать скрытые за ними щели и полости.

Визуальному осмотру подлежат не только предметы интерьера помещения, но также предметы, являющиеся содержимым ящиков столов, шкафов и другой мебели, карманов хранящейся в помещении одежды и других ёмкостей.

Осмотр предмета начинается с оценки возможности его использования как объекта для внедрения противником ЗУ. В случае положительной оценки проверяется подлинность предмета для исключения вероятности его подмены и выявляются следы возможного вскрытия предмета противником.

Визуальный осмотр может выявить практически все типы подбрасываемых ЗУ и подавляющее большинство ЗУ, требующих незна-

чительного времени для их установки. Для некоторых видов ЗУ визуальный осмотр является единственным способом их обнаружения.

Обнаружение ЗУ не должно стать причиной поверхностного выполнения остальных предусмотренных планом поисковых работ, тем более их свёртывания и прекращения. Следует помнить о таком общеизвестном тактическом приёме, как «отвлекающий маневр», более известный среди сотрудников спецслужб под названием «отвлечение на негодный объект». Весьма вероятно, что противник установил не одно, а два или даже несколько дублирующих друг друга ЗУ как раз в расчёте на то, что после обнаружения одного из них поисковая бригада ослабит или вообще свернёт дальнейший поиск. Уверенность в «чистоте» проверяемого помещения может дать только полное и тщательное выполнение всех запланированных поисковых работ.

Обследование с помощью поисковых средств. Выявление демаскирующих признаков закладочных устройств обычно проводят последовательно, поочерёдно проверяя наличие излучения:

- автономных радиомикрофонов и телефонных радиоретрансляторов;
- камуфлированных радиомикрофонов, питающихся от электросети;
- радиостетоскопов;
- скрытых видеокамер с радиоканалом;
- пространственного высокочастотного облучения;
- радиозакладок в ПЭВМ и других электронных приборах;
- выявление неработающих во время проверки ЗУ.

Акустический фон для активизации радиозакладок с акустопуском создается размещением в контролируемом помещении тестового источника звука. В качестве такого источника можно использовать магнитофон с хорошо известной музыкальной или речевой фонограммой. Не рекомендуется использовать в этих целях радиоприемник или телевизор, так как создаваемый ими звуковой сигнал, переизлучаемый радиозакладкой, может совпасть с радиосигналом выбранной вещательной станции. Выбор громкости тестового звукового сигнал определяется как размерами помещения, так и чувствительностью микрофона радиозакладки. Обычно такие микрофоны уверенно воспринимают звук средней громкости с расстояния порядка 10 метров.

Поиск радиомикрофонов. Современные условия поиска и необходимость использования аппаратно-програмных комплексов для выявления ЗУ с закрытием канала передачи привело к необходимости изменения методики выявления ЗУ с помощью поискового оборудования. Наиболее рациональным вариантом проведения поиска радиомикрофонов с использованием поискового оборудования будет следующий порядок работ.

Перед началом выявления устройств несанкционированного получения информации, работающих по радиоканалу, необходимо включить програмно-аппаратный комплекс в контролируемом помещении в режим обзора. На мониторе появятся спектрограммы активных сигналов, выявленных в ходе проведения предварительного радиомониторинга и отнесенные оператором к подозрительным или неизвестным излучениям. С помощью критериальной базы комплекса определить, что источник излучения находится в контролируемом помещении. Затем с использованием индикаторов поля или универсальных приборов типа «Пираньи» осуществить локализацию и обнаружение источника излучения.

Порядок действий при выявлении ЗУ рассмотрим с применением селективного индикатора поля RAKSA-120. Панорамный селективный индикатор поля RAKSA-120 предназначен для обнаружения в ближней зоне и локализации радиопередающих устройств, использующихся для негласного съема информации, включая мобильные телефоны и устройства Bluetooth. Индикатор поля работает по принципу скоростного сканирующего приемника с широкой полосой канала приема. В индикаторе поля RAKSA-120 предусмотрены режимы охраны, обзора, поиска и поиска с вычитанием спектра.

В охранном режиме прибор в реальном времени без участия оператора отслеживает появление опасных радиосигналов. В этом режиме реализован оригинальный алгоритм адаптации к электромагнитной обстановке, игнорирующий стационарные помехи. Для каждого типа сигнала может быть установлен пороговый уровень. Обнаружение любого из типов сигнала может быть вообще отключено.

В режиме обзора происходят непрерывное измерение текущего уровня выбранного сигнала и циклическая перестройка по всему диапазону частот. Этот режим наиболее целесообразно использовать для локализации источников радиосигналов в сложной радиоэлектронной обстановке. Информация, выводимая на дисплей в данном режиме, позволяет оператору определить, есть ли в данный момент на дисплее сигнал с частотой, определенной на мониторе аппаратно-програмного комплекса как подозрительная. Результаты отображаются на дисплее. При наличии сигнала с такой частотой, необходимо настроить индикатор поля на частоту несанкционированного источника излучения (рис. 5.8) из проверяемого помещения. Плавно перемещаясь по обследуемому помещению, добиться

Рис. 5.8. Индикация обнаруженных сигналов на RAKSA-120

отображения на дисплее прибора максимальной величины сигнала источника излучения. По максимуму излучения визуально обнаружить источник излучения.

При отсутствии на дисплее прибора частоты, обнаруженной программно-аппаратным комплексом, целесообразно кроме индикатора поля использовать сканирующий приемник типа «Скорпион 3.5». Методика работы с данным прибором основана на возможности прибора работать на две антенны. При работе на две антенны необходимо настроить прибор на обнаруженное излучение из проверяемого помещения и по равносигнальной зоне определить направление на источник излучения. После чего, сменив направление контроля, повторить операцию засечки и определить пеленг источника сигнала с другого направления. Точка пересечения двух лучей покажет примерный район нахождения источника излучения. Затем с помощью индикатора поля, приблизившись к точке излучения и плавно перемещаясь по проверяемому помещению в районе возможного расположения ЗУ, локализовать его, обследуя ограждающие поверхности и места возможного размещения. По увеличению мощности сигнала требуемой частоты локализовать его по максимуму излучения.

Порядок поиска работающих радиомикрофонов при отсутствии данных радиомониторинга. Некоторые индикаторы поля, такие как ST-107, ST-110, требуют предварительной настройки перед проведением поиска. Подготовка поискового прибора (после проверки его работоспособности в данном режиме) заключается в установке нулевого порога обнаружения (ПО), что является, фактически определяющим для успешного проведения работ. Нулевой ПО должен соответствовать реальному фону контролируемой территории. Занижение значение ПО приведёт к частым ложным срабатываниям индикации, а его завышение — к вероятному пропуску сигнала радиозакладки. И то, и другое значительно усложняет работу оператора, увеличивает время и снижает достоверность результатов проверки.

Условия необходимые для установки «нулевого» порога:

- установка порога производится за пределами проверяемого помещения;
- во время настройки порога недопустимо использование радиостанций, радиотелефонов и других радиоизлучающих средств;
- нельзя приближать антенну прибора к включенным ПЭВМ и другим средствам оргтехники;
- не допускается контакт антенны прибора с металлическими предметами и проводами как возможными источниками переизлученных высокочастотных сигналов.

Настройка прибора производится в одном из ближайших к проверяемому помещений, в котором, предположительно, уровень фона

существенно не отличается, а установка радиозакладок либо невозможна, либо нецелесообразна. В качестве таких помещений обычно рассматривают помещения другого предназначения, но расположенные на том же этаже и с оконными проемами, выходящими на ту же сторону здания.

После установки нулевого порога прибор перемещают в проверяемое помещение без выключения питания, так как последующее его включение приводит к автоматической установке порога уже применительно к новым условиям электромагнитной обстановки.

При отсутствии ограничений на скрытность проведения работ наилучший эффект дает сочетание амплитудного метода и метода акустозавязки. При проведении скрытного поиска целесообразно использовать амплитудный метод с прослушиванием детектированных сигналов через головные телефоны. При поиске особое внимание обращается на радиоизлучения в диапазоне 60...640 МГц, который является наиболее типичным для использования закладочными устройствами.

Методика поиска заключается в планомерном и тщательном обходе контролируемого помещения (объекта) с движением вдоль стен и обследованием мебели и других расположенных в нем предметов. Поиск целесообразно начинать с применением телескопической антенны. При обходе антенну необходимо ориентировать в разных плоскостях, совершая плавные, медленные повороты основного блока и добиваясь максимального уровня сигнала. Антенну прибора целесообразно держать на расстоянии не более 20...25 см от обследуемых поверхностей и предметов. При отсутствии ограничений на использование метода акустозавязки динамик встроенного громкоговорителя прибора следует ориентировать в сторону обследуемых поверхностей и предметов.

При приближении антенны прибора к месту размещения радиозакладки напряженность электромагнитного поля возрастает, повышается и уровень сигнала. Для визуальных индикаторов с превышением уровнем сигнала установленного нулевого порога увеличивается количество окрашенных секторов индикаторов уровня (или повышается значения показаний стрелочных индикаторов), для звуковых индикаторов возрастает уровень звукового сигнала (или увеличивается частота щелчков звуковой сигнализации).

При приближении поискового прибора к радиомикрофону с частотномодулированным сигналом будет увеличиваться количество окрашенных секторов индикатора уровня сигнала (или показаний стрелочного индикатора). Радиочастотомер осуществляет захват частоты и показывает ее значение по результатам измерений. При использовании режима акустозавязки при уменьшении громкости увеличивается порог срабатывания, за счет чего сужается зона обследования и место установки радиозакладки локализуется с погрешностью в пределах до

10...15 см. Дополнительные возможности, прежде всего по классификации радиоизлучений ЗУ с открытым каналом, дает периодическое включение режима прослушивания демодулированного сигнала.

Однако для поиска закладочных устройств с маскированным радиоканалом приходится использовать только амплитудный метод. Дополняющим здесь может быть простой прием. Если выключить источник тестовой фонограммы и создать в проверяемом помещении короткий резкий звук (сильный хлопок, удар по крышке стола или металлическому предмету), то можно зафиксировать характерные изменения демодулированного сигнала «на слух», изменения осциллограммы и спектрограммы (при применении прибора «Пиранья»).

При применении радиозакладки с цифровыми методами модуляции индикация частоты принимаемого сигнала (при использовании радиочастомера) будет случайной. Идентификацию повышения уровня сигнала (при приближении к радиозакладке) можно осуществить с помощью индикации пиковой осциллограммы, которую можно зафиксировать на нижнем индикаторе (при применении прибора «Пиранья»).

В случае применения в качестве радиозакладки телефонов стандарта DECT или GSM некоторые поисковые приборы (RAKSA-120, ST-107, ST-110, «Пиранья» и др.), помимо индикации уровня повышения сигнала, дают информацию на индикаторе в виде надписей DECT или GSM.

Поиск телефонных радиоретрансляторов. Методика поиска сводится к следующему алгоритму. Поиск проводится в два этапа. Для активизации телефонных радиоретрансляторов снять трубку телефонного аппарата. Сначала проверяются телефонные аппараты. Установленный в аппарате радиоретранслятор проявляется точно так же, как и радиомикрофон. При приближении антенны поискового прибора к такому телефонному аппарату срабатывают средства звуковой индикации и визуальный индикатор уровня сигнала. При переключении прибора в режим аудиоконтроля в динамике или в головных телефонах прибора прослушивается либо непрерывный, либо прерывистый тональный сигнал телефонной станции. В ряде случаев при приближении микрофона телефонной трубки к динамику прибора может возникнуть эффект акустозавязки. Не рекомендуется проверять телефонные аппараты в режиме громкоговорящей связи (если он предусмотрен), так как в этом случае может возникнуть ложная акустозавязка между микрофоном и динамиком самого аппарата.

Далее поиск осуществляется обходом помещения вдоль абонентской телефонной линии и выявлением на ней мест с возрастанием (максимумом) уровня радиосигнала. При обходе антенну прибора необходимо ориентировать в разных плоскостях на минимально возмож-

ном расстоянии от линии. Практически всегда существует необходимость проверки линии вплоть до основного распределительного щита. Особое внимание следует обращать на распределительные коробки и места, где линия проложена скрытой проводкой. Установленные на линии закладочные устройства локализуются, в основном, амплитудным методом, дополняемым проверкой на акустозавязку.

Поиск сетевых радиомикрофонов. Методика поиска сетевых радиомикрофонов аналогична. Для их активизации включается тестовый источник звука и с помощью поисковых приборов проверяются места вероятного нахождения сетевых радиомикрофонов, прежде всего в розетках и переключателях. Проверяется бытовая электротехника, находящаяся в контролируемом помещении. Для этого необходимо поочередно включать имеющиеся осветительные приборы с лампами накаливания и подключать к розеткам электросети шнуры питания бытовых приборов. Последовательно проводится обследование каждого из вновь подключенных средств.

Поиск радиостетоскопов. Методика поиска радиостетоскопов имеет особенности, обусловленные способом их применения — установке вне контролируемого помещения. Для обнаружения сигнала радиостетоскопов необходимо обследовать все реально доступные внешние поверхности ограждающих помещение конструкций. Затем проверяются выходящие из проверяемого помещения коммуникации.

В подавляющем большинстве радиостетоскопы используют открытый радиоканал. Это дает возможность анализа принятого сигнала «на слух» в режиме аудиоконтроля. При проверке ограждающих конструкций антенну поискового прибора следует располагать на минимально возможном расстоянии от обследуемых поверхностей, так как радиус зоны обнаружения сигнала от радиостетоскопа обычно меньше, чем от радиомикрофонов. При проверке трубопроводных коммуникаций необходимо выполнять эти же рекомендации, но не допускать контакта антенны с металлическими поверхностями.

Локализация местонахождения радиостетоскопов осуществляется амплитудным методом в смежных помещениях. Для повышения достоверности обнаружения при наличии соответствующих поисковых приборов (например, АПКР, «Пиранья») можно использовать режимы осциллограммы и спектрограммы.

Поиск скрытых видеокамер. Методика поиска скрытых видеокамер с радиоканалом передачи изображения (часто и звука) сопряжена с некоторыми трудностями, которые определяются сходством сигнала видеопередатчика с сигналами яркости передатчиков телевизионного вещания и работой значительного количества этих устройств в диапазоне (от 1200 до 5600 МГц).

При обнаружении сигнала первой является задача его распознавания по критерию «внешний–внутренний». Для чего в контролируемом помещении необходимо закрыть окна шторами или жалюзи, оставив включенным внутреннее освещение. Далее несколько раз включается и выключается искусственное освещение. При наличии скрытой видеокамеры с радиоканалом передачи изображения и включенном режиме аудиоконтроля должны прослушиваться отчетливые изменения тона продетектированного сигнала. При использовании для выявления видокамер передающих информацию по радиоканалу аппаратно-програмных комплексов возможно получение на мониторе комплекса изображения объекта съемки видеокамеры, а также изменение структуры сигнала по осциллограмме при включении и выключении освещения.

Если результаты такой проверки положительны, то сигнал уверенно можно отнести к категории внутренних, создаваемых передатчиком видеокамеры, так как изменение освещенности помещения на параметры сигнала телевизионного вещания не влияет. Кроме того, полученное изображение на мониторе (рис. 5.9, см. также рис. 2.42) позволит оператору определить расположение скрытой видеокамеры.

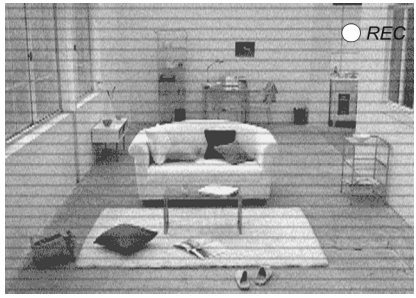


Рис. 5.9. Вариант изображения от скрытой беспроводной видеокамеры

Принципиально передатчики видеокамер могут работать на частотах до 2400 МГц, однако в последнее время появились видеокамеры, передающие сигналы по радиоканалу на частотах более 5000 МГц. Обнаружение сигнала (похожего на сигнал яркости) на частотах вне диапазона телевизионного вещания практически однозначно свидетельствует о работе передатчика скрытой видеокамеры. Локализация таких средств осуществляется амплитудным методом.

При применении комплекса «Спектр-Professional» возможно выявление видеокамер, работающих по радиоканалу, также и на частотах более 5000 МГц. С помощью встроенной системы видеозахвата данный комплекс выводит на экран управляющего компьютера продетектированное изображение от скрытых беспроводных видеокамер. Обнаруженный «опасный» сигнал может быть записан на жесткий диск компьютера для последующего анализа.

Однако такого рода поисковые мероприятия не позволят локализовать видеокамеры, передающие информацию по проводам, что вызывает необходимость более детально рассмотреть данный вопрос.

Современное состояние средств получения видеоинформации позволяет сделать вывод, что по своим возможностям современные видеокамеры стали грозным оружием при решении задач негласного получения видео- и аудиоинформации. Это привело к тому, что задача выявления скрытых видеокамер в настоящее время выходит на одно из первых мест. А следовательно, необходимо более глубоко рассмотреть вопросы, касающиеся выявления такого рода ЗУ.

Прежде чем перейти к методике поиска, целесообразно рассмотреть и дать краткий анализ демаскирующих признаков современных видеокамер и аппаратуры, предназначенной для выявления скрытых видеокамер по их демаскирующим признакам.

Итак, современные видеокамеры условно можно разделить на две большие группы: передающие информацию по проводам и по радиоканалу. И те и другие могут работать как от сети, так и от автономных источников питания.

Для передачи видеоинформации объектив видеокамеры, независимо от способа передачи информации, должен быть открыт. Следовательно, наша задача найти те демаскирующие признаки, по которым можно гарантированно определить наличие объектива в проверяемом помещении.

Так как основной задачей любого объектива (независимо от его размера) является передача сфокусированного изображения на электронную матрицу или систему призм для дальнейшей обработки и передачи видеосигнала, то в их состав обязательно входят фокусирующие линзы. При направлении на линзу светового потока он переотражается ей и оператор визуально наблюдает это переотражение в виде светящейся точки или кольца в зависимости от размера и типа объектива. Вот на этом свойстве переотражения направленного на объектив светового потока и основано действие оптических обнаружителей видеокамер.

В настоящее время на российском рынке представлено достаточное количество таких приборов, отличающихся своими характеристиками и ценовым диапазоном. К таким приборам относятся: «Оптик-2», «Прометей», «Стилет», «Хабл», «СтопКам» и широкий ряд приборов китайского производства.

Принцип действия этих обнаружителей банально прост. В их состав в качестве основного элемента входит источник света, формирующий яркий световой поток, отличный от дневного света. Это может быть красный, зеленый, синий или их комбинация. При направлении светового потока на место расположения объектива оператор будет визуально наблюдать светящуюся точку или кольцо того же цвета. Таким образом, задача оператора сводится к необходимости определения, от какого источника идет переизлучаемый сигнал, так как

свойствами переотражения, кроме объективов, обладают различные зеркальные поверхности, хрустальная посуда и т. д. Но оператор всегда имеет возможность подойти и убедиться, от какого источника идет световой сигнал.

Применения данного метода выявления скрытых видеокамер дает практически гарантированный результат их обнаружения, но связано с определенными трудностями, а именно:

- необходимостью осмотра достаточно большой площади проверяемого помещения, что достаточно утомительно;
- возможностью пропуска отраженного сигнала при длительной работе оператора из-за утомляемости и однотонности поиска.

Обнаружение видеокамер, передающих видеоинформацию по радиоканалу, основано на том, что при передаче видеосигнала в эфире появляется радиоэлектронное излучение в том частотном диапазоне, в котором работает излучающая видеокамера. Оператор, при наличии соответствующей аппаратуры, фиксирует это излучение и по его максимуму, используя амплитудный метод, может его локализовать. К таким приборам, позволяющим реализовать данный метод, относятся «Амулет», «Айрис» (IQ-series).

Данный метод позволяет выявлять видеокамеры, работающие по радиоканалу, облегчает работу оператору, но не обеспечивает гарантируемое обнаружение всех видеокамер, так как постоянно совершенствуются стандарты передачи видеосигналов, изменяется частотный диапазон и другие характеристики, что приводит к необходимости постоянного отслеживания данных изменений и внесения корректив в программную оболочку приборов.

Применение современных аппаратно-программных комплексов для поисковых работ также позволяет выявлять и локализовать видеокамеры, передающие информацию по радиоканалу. К таким комплексам относятся аппаратно-программные комплексы «Касандра» и серии «Спектр».

Последней разработкой в этой области стала разработка обнаружителя скрытых видеокамер SEL SP-102 «Аркам» (рис. 5.10).

Рис. 5.10. Обнаружитель скрытых видеокамер SEL SP-102 «Аркам»

Обнаружитель скрытых видеокамер SEL SP-102 «Аркам» предназначен для дистанционного обнаружения в помещениях и предметах скрытых видеокамер, находящихся в активном состоянии, т. е. ведущих съёмку. «Аркам» позволяет находить камеры вне зависимости от их камуфляжа и способа передачи видеоинформации. Прибор в состоянии обнаруживать как

обычные (проводные) камеры, так и камеры, передающие информацию по радиоканалу. Наличие или отсутствие передатчика не влияет на работу обнаружителя. Действие прибора основано на анализе определённых участков электромагнитного спектра на предмет излучений, свойственных только видеокамерам. «Аркам» производит анализ электромагнитной обстановки в исследуемой зоне на наличие паразитных излучений от работающих видеокамер. Параметры паразитных излучений индивидуальны для каждого типа камеры, и их комбинации представляют электромагнитный «портрет», присущий данному типу. В настоящее время на территории России широко применяются порядка 10 типов аналоговых и аналого-цифровых видеокамер с параметрами (размеры, энергопотребление, конструкция объектива), которые позволяют производить скрытую установку. Обнаружив подозрительное излучение, похожее на излучение камеры, хранящееся в базе данных прибора, «Аркам» исследует и анализирует найденные частоты по 10 алгоритмам, чтобы исключить возможность ошибки. При обнаружении видеокамеры прибор отображает это на сенсорном ЖК экране. При этом отображается уровень найденного излучения, что позволяет производить поиск камеры в окружающей обстановке.

Таким образом, «Аркам» не требует пристального монотонного осмотра всех плоскостей помещения, а позволяет в течение считанных секунд определить наличие скрытой видеокамеры и затем попытаться найти её. Однако, в отличие от обнаружителей видеокамер, работающих по оптическому принципу, применение «Аркама» не гарантирует обнаружение видеокамер, находящихся в режиме ожидания и имеющих характеристики, отличные от тех, которые занесены в память прибора.

Рис. 5.11. Тепловизор

В настоящее время появилось еще одно направление поисковых работ, позволяющее по косвенным признакам определить наличие в ограждающих конструкциях скрытых видеокамер. Данное направление связано с распространением тепловизоров. Применение ручных тепловизоров (рис. 5.11) позволяет определить тепловую картинку от работающей видеокамеры, находящейся в ограждающей конструкции, а затем оператор визуально или с помощью оптических обнаружителей локализует видеокамеру.

Поиск пространственного высокочастотного облучения. В данном случае необходимо выявить факт создания этого канала утечки информации, т. е. обнаружить наличие высокочас-

тотного облучения, а затем убедиться в наличии отклика на зондирующий высокочастотный сигнал.

Остронаправленный луч электромагнитной энергии может быть сформирован только на очень высоких частотах (800...900 МГц и выше). Особенности распространения радиоволн этого диапазона (необходимость «прямой видимости» между источником излучения и облучаемыми предметами) определяют в качестве основных путей их проникновения в контролируемое помещение прежде всего оконные проемы. Переизлучающими объектами могут быть обычные для данного помещения технические средства с микрофонным эффектом (динамики бытовых громкоговорителей, акустические системы даже выключенной аудиоаппаратуры, телефонные аппараты с электрическим звонком и т. п.). Переизлученный на частотах высших (чаще всего второй или третьей) гармоник сигнал локализуется в непосредственной близости от облучаемых предметов и имеет модуляцию акустическим фоном помещения.

Для выявления факта высокочастотного облучения поочередно обследуют потенциально опасные оконные проемы. Для этого следует поднести антенну к внутреннему стеклу на расстояние 5...10 см, зафиксировать уровень и частоту наиболее мощного сигнала. Включить режим аудиоконтроля и «на слух» определить наличие и особенности демодулированного сигнала. При наличии соответствующих поисковых приборов можно оценить стабильность частоты излучения. Затем перейти в любое из соседних помещений (ориентированных окнами в ту же сторону) и повторить проверку в районе каждого из его оконных проемов.

Высокочастотное облучение вполне вероятно, если:

- частота принимаемого сигнала лежит (или очень близка) в пределах указанного диапазона;
- стабильность частоты высокая;
- модуляция сигнала отсутствует;
- в соседних помещениях уровень принимаемого сигнала существенно меньше.

Для выявления источников переизлучения, находящихся в контролируемом помещении, необходимо тщательно обследовать каждый из потенциально опасных предметов, размещая антенну прибора в непосредственной близости к нему. Основанием для принятия конечного решения о наличии в помещении переизлучающих предметов являются визуальные показания индикатора частотомера, а также результаты прослушивания в режиме аудиоконтроля. При этом основными признаками пространственного высокочастотного облучения можно считать фиксацию номинала частоты, кратного максимум

третьей гармонике облучающего сигнала, и идентификацию звукового сигнала с акустическим фоном помещения.

Выявление пассивных и полупассивных ЗУ, использующих высокочастотное навязывание, в настоящее время вышло на новый уровень. Использование специальных комплексов позволяет с высокой степенью вероятности выявлять резонансные переизлучатели (эндовибраторы и другие вторичные излучатели) в технических средствах обработки информации, средствах оргтехники, помещениях, предметах интерьера и т. п.

Принцип работы комплекса основан на облучении обследуемых объектов высокочастотным электромагнитным полем (от 100 МГц до 3 ГГц) при одновременном акустическом воздействии с последующим приемом переизлученного (отраженного) сигнала и его анализом на наличие модуляции, обусловленной этим акустическим воздействием.

В состав комплекса входят:

- управляемый высокочастотный генератор;
- приемная и передающая антенны;
- акустический излучатель;
- широкодиапазонный эталонный переизлучатель, который содержит три переизлучающие структуры с резонансными частотами 500, 1000 и 2250 МГц.

Управление аппаратурой и обработка результатов осуществляется с помощью многофункционального комплекса радиоконтроля «Омега».

Комплекс может работать в автоматическом и ручном режимах. В автоматическом режиме комплекс облучает исследуемый объект высокочастотным электромагнитным полем и выполняет обнаружение и измерения относительных уровней модуляционных сигналов в переизлученных колебаниях, обусловленных акустическим воздействием на объект. Исследования выполняются при последовательном сканировании заданного диапазона радиочастот с равномерным или переменным шагом по частоте с параметрами, которые предварительно вводятся при настройке программы. Для исключения влияния фазового шума генератора и гетеродинов приемника обнаружение и измерение уровней модуляционных сигналов выполняется с помощью анализатора спектра огибающей, полоса обзора которого может расширяться до 100 кГц, что позволяет регистрировать высокочастотные модуляционные компоненты в спектре отраженного сигнала. После завершения сканирования все результаты сохраняются в файле и могут быть представлены в виде документального отчета.

В автоматическом и полуавтоматическом режимах управление аппаратурой и обработка результатов осуществляется с помощью комплекса «Омега». При управлении аппаратурой с помощью автоном-

ной ПЭВМ возможно проведение работ в ручном режиме. При этом во всем рабочем диапазоне обеспечивается заданная чувствительность и максимальное значение подводимой к антенне мощности облучаемого сигнала.

«Омега-А (АМ)» отличается высокой равномерностью выходной мощности по диапазону, низкими фазовыми шумами и полной автоматизацией процессов измерения.

Генератор управляется от внешнего компьютера или контроллера через стандартные последовательные интерфейсы: RS-232 и PS/2.

Выявление утечки информации по проводным линиям различного назначения. Основными видами проводных линий, подлежащих приборной проверке, являются линии электросети, абонентские телефонные линии и линии систем пожарной и охранной сигнализации. Методика проверки данных проводных линий практически одинакова. Порядок подключения к ним зависит от используемой аппаратуры и, в большинстве своем, осуществляется с использованием адаптеров и различных щупов, конфигурация которых зависит от характера проверяемой линии. Анализу подвергается общий диапазон от 0 до 15 МГц, при этом:

- проводится подготовка контролируемого помещения для осмотра (проверяется соответствие количества и назначение реально существующих в нём проводных линий представленным схемам их прокладки);
- выбираются наиболее удобные наконечники к щупам применительно к типу и особенностям имеющихся проводных линий.

В ходе проверки наибольшее внимание уделяется диапазону 40... ...2500 кГц как наиболее типичному для закладочных устройств, питающихся от напряжения проводных линий и передающих перехваченную информацию по проводам. Значительно реже встречаются закладочные устройства с частотами около 7 МГц и выше. Для обеспечения гарантированной надёжности обнаружения закладочных устройств по частоте верхняя граница диапазона сканирования в приборах должна быть на уровне 15 МГц.

Рекомендуется следующий порядок действий оператора.

Сначала сканируется диапазон до 10 МГц. После завершения 2–3-х циклов сканирования устанавливается верхняя граница диапазона сканирования на уровне 15 МГц. В процессе сканирования внимательно изучаются наиболее характерные особенности изображения панорамы и определяются наличие частотных составляющих, превышающих уровень общего фона.

При необходимости частотный диапазон разбивается на отдельные интервалы и их сканирование осуществляется отдельно, с тщательным изучением наиболее интенсивных составляющих частотного

спектра. Проведение поиска может дополняться проведением анализа сигналов в режимах осциллограммы и спектрограммы, так как в них проявляется более детальная характеристика параметров исследуемого «опасного» сигнала.

Если контролируемое помещение проверяется регулярно, то целесообразно сохранить в энергонезависимой памяти панораму (осциллограмму, спектрограмму) необходимых частотных интервалов.

При проверке проводных линий необходимо учитывать специфические особенности линий каждого вида.

Проверку на наличие закладочных устройств в электросети целесообразно начинать с сетевых розеток. Для уменьшения уровня фона отключить (с отсоединением от розеток) все электроприборы и аппаратуру, размещённую в контролируемом помещении.

После подключения поискового прибора к сети (можно использовать для этого любую из розеток, находящихся в контролируемом помещении) необходимо провести анализ изображения панорамы. Если обнаружен сигнал, содержащий признаки модуляции акустикой помещения, то для локализации его источника может быть использован метод акустозавязки при поочерёдном подключении ко всем розеткам в проверяемом помещении.

Аналогичную проверку провести на элементах линий, питающих электроосветительные приборы.

После проверки силовых линий и линий, питающих осветительные приборы, необходимо проверить тройники, удлинители и другие электропотребляющие средства, поочерёдно подключая их к электросети.

Проверка проводных линий систем пожарной и охранной сигнализации, а также линий неизвестного предназначения аналогична проверке линий электросети, так как аналогичны сами технические средства, используемые на этих коммуникациях.

Проверка телефонных линий. Сложность телефонных систем, их разветвлённость создают повышенные объективные трудности при их обследовании. Изучая опыт проведения проверок, можно сделать вывод, что чем сложнее телефонная система, тем проще противнику установить ЗУ. В целом, процесс исследования телефонного оборудования включает следующие мероприятия [58]:

1. Проведение предварительного контроля и исследования с целью определения сложности системы, а также типа, необходимого для контроля, оборудования.

2. Подготовка плана по проведению контроля.

3. Визуальная проверка оснащения, проводов и кабелей телефонной системы. Проверка всей системы с точки зрения её соответствия спецификации.

4. Все провода (в парах и раздельно) каждой входной линии должны быть проверены акустическим усилителем и соответствующими приёмниками радиочастоты с целью обнаружения передачи во время нормальной работы системы.

5. В связи с тем, что многие контактные колодки имеют параллельные соединения, необходимо точно удостовериться, все ли провода ведут к колодке, которая проверяется в настоящий момент, и нет ли альтернативных линий. В этом случае необходимо обследовать телефонные кабели на всём протяжении и окончания в колодках.

6. Необходимо провести тщательное исследование при помощи аналитической аппаратуры и соответствующих приёмников радиочастоты. Каждый провод нужно проверить со всеми остальными проводами и заземлением.

7. Необходимо выполнить обследование с помощью приборов всех устройств, приводящих в действие данное оборудование. Необходимо провести осмотр всех деталей телефонной системы. Он должен включать демонтаж аппаратов, соединений, а также присоединённых приборов.

8. Кроме того, при проверке абонентских телефонных линий, помимо проводимых, описанных выше мероприятий, телефонные линии проверяются на наличие линейного высокочастотного навязывания. Признаком факта линейного высокочастотного навязывания является наличие в линии немодулированного стабильного зондирующего сигнала на частотах не ниже 150 кГц. При этом порядок подключения приборов и процедура анализа не отличаются от изложенного применительно к проверке линий электросети.

Изложенные положения позволяют сделать вывод, что исследование линий связи на наличие закладочных устройств — очень трудная и дорогостоящая задача, требующая применения различных приборов. Сложности заключаются в том, что закладочное устройство может быть установлено на большом расстоянии от телефона, а методы съёма информации очень разнообразны.

При этом необходимо помнить, что любое контактное подключение к линии приводит к изменению её электрических параметров, выявление которых требует применения сложной аппаратуры. Для регистрации электрических параметров линии применяют телефонные анализаторы, с помощью которых можно измерить напряжение, ток линии, сопротивление и ток утечки и, сравнив затем с параметрами линии в нормальном состоянии, сделать заключение о наличии и характере (параллельное или последовательное подключение) несанкционированных подключений. Особенности применения данных приборов связаны с тем, что перед их применением необходимо знать параметры нормальной линии, которые при плохом (это бывает очень

часто) монтаже могут произвольно меняться от погодных и других внешних факторов в очень широкомдиапазоне. Пользователям защищённых телефонных аппаратов можно посоветовать чаще обращать внимание на дисплей прибора защиты телефонной линии, который регистрирует напряжение линии. Целесообразно завести журнал, в который ежедневно заносить показания дисплея прибора, а затем анализировать эти значения.

Другие наиболее дорогие приборы — кабельные локаторы. Принцип действия данных приборов заключается в посылке коротких импульсов в линию. Достигая точки неоднородности в линии (контактное подключение), импульс отражается и регистрируется прибором. По времени задержки отраженного сигнала можно определить расстояние до нелинейности. Трудности в применении данных приборов связаны, как правило, с их большими габаритами и весом. Часть приборов требует обесточивания линии и имеют относительно высокую стоимость. Кроме того, наличие скруток на линии зачастую воспринимается прибором как нелинейность. Такое разнообразие приборов для проверки телефонных линий вызывает необходимость ознакомиться с основными характеристиками наиболее распространенных приборов для контроля телефонных линий.

Рис. 5.12. Универсальный анализатор линейных коммуникаций «Улан»

Универсальный анализатор линейных коммуникаций «Улан» (рис. 5.12) предназначен для проверки любых проводных коммуникаций, таких как телефонные линии, сети 220 В, свободные пары и т. п., на наличие гальванически подключенных к ним цепей согласования и питания устройств передачи информации.

Прибор позволяет обнаружить и идентифицировать в линиях АТС без отключения напряжения:

- последовательные подключения с эквивалентным сопротивлением от 30 Ом и выше;
- параллельные подключения в режиме «ожидание вызова» с токами потребления от 0,1 мА и выше;
- параллельные подключения в режиме «снятая трубка» с токами потребления от 0,1 мА и выше;
- высокочастотные сигналы в линии 0,02...30 МГц при симметричном (ВЧ подкачка) и несимметричном (ВЧ навязывание) подк-

лючении с эффективным напряжением от 10 мВ и выше;
- низкочастотные сигналы в линии 20...20000 Гц с эффективным напряжением от 10 мВ и выше;

в линиях без напряжения:
- параллельные подключения с активным сопротивлением от 100 Мом и ниже;
- последовательные подключения с активным сопротивлением от 1 Ом и выше;
- параллельные подключения через конденсатор с постоянной времени от 1 мс и выше;
- наличие элементов с выраженной нелинейностью от 5 % и выше в диапазоне напряжений 0...100 В;
- наличие реактивных элементов с емкостью более 10 % от собственной емкости линии и индуктивностью более 1 Гн;

в линиях сети 220 В:
- «сторожевые устройства» с током потребления от 0,1 мА и выше.

Точность измерения перечисленных параметров не хуже 10 %.

Прибор имеет ряд дополнительных функций:
- измерение напряжения постоянного и переменного токов в проверяемой линии;
- прослушивание аудиосигналов в линии на головные телефоны;
- поиск трассы прокладки проверяемой линии в строительных конструкциях.

Прибор может работать как в ручном, так и в автоматическом режимах, а также в автономном режиме контроля выбранных параметров по заданному сценарию с возможностью накопления информации и последующей передачей ее в персональный компьютер для автоматизированного анализа и обработки.

Анализатор проводных коммуникаций LBD-50 (рис. 5.13) предназначен для поиска несанкционированных гальванических подключений. В анализаторе реализован комплекс методов обнаружения: исследование нелинейных преобразований сигналов, подаваемых в линию, анализ переходных процессов в линии, измерения параметров линий (ток утечки, сопротивление изоляции).

Анализатор обнаруживает подключения устройств, предназначенных для перехвата информации, передачи материалов перехвата, обеспечения электропитанием.

Алгоритм обследования, заложенный в анализаторе, исключает срабатывание защитных сторожевых схем в объектах поиска.

Технические характеристики: тип и состав обнаруживаемых подключений — параллельные и последовательные нелинейные элементы, R-, C-элементы; диапазон измерения токов утечки от 0,1 до 200 мА;

Рис. 5.13. Анализатор проводных коммуникаций LBD-50

Рис. 5.14. Измеритель неоднородностей линий типа Р5-10

диапазон измерения сопротивления изоляции от 100 кОм до 20 Мом; длина анализируемой линии от 800 до 50 м в зависимости от погонной емкости; питание — сеть переменного тока 220±20 В частотой 50 Гц; габариты 500×400×140 мм; масса 4 кг.

Входящие в комплект кабели и принадлежности обеспечивают возможность подключения к анализируемым линиям практически во всех возможных ситуациях, что позволяет проводить обследование любых проводных коммуникаций независимо от их назначения.

Комплект прибора содержит специальный трассоискатель, позволяющий бесконтактным способом найти обследуемую линию в распределительном шкафу, жгуте и т. п.

Измеритель неоднородностей линий Р5-10 (рис. 5.14) является универсальным малогабаритным прибором со сменными блоками питания, обеспечивающими работу от сети постоянного тока напряжением от 10 до 15 В и от 22 до 30 В, переменного тока напряжением 220±22 В частотой 50, 400 Гц и от автономного источника питания.

Прибор может работать в полевых условиях при температуре от −30 до 50 °С и относительной влажности до 98 % при температуре до 35 °С.

Измеритель Р5-10 предназначен для:

- обнаружения повреждения и определения его характера (обрыв, короткое замыкание);
- обнаружения сосредоточенной неоднородности волнового сопротивления (асимметрия в проводах, нарушение контакта, вставки, неоднородности и др.);
- определения расстояния до повреждения или неоднородности.

Измеритель Р5-10 может быть использован для контроля состояния кабелей, прогнозирования неисправностей в них, измерения их длины и симметрирования.

Чувствительность измерителя обеспечивает просмотр линий с затуханием до 80 дБ в полосе 3,5...7 кГц. Минимальная длина линии 5 м.

Комплекс для исследования сигналов в проводных линиях «Сириус» (рис. 5.15) предназначен для обнаружения и анализа сигналов в проводных линиях и в подключенных к ним электронных устройствах, возникающих за счет как прямого формирования, так и акустоэлектрических преобразований.

Рис. 5.15. Комплекс для исследования сигналов в проводных линиях «Сириус»

Исследование сигналов проводится методами прямого векторного спектрального анализа и анализа модулирующих сигналов с использованием метода ВЧ навязывания. В комплексе реализованы: широкий диапазон частот исследуемых сигналов; векторный спектральный анализ в различных промежуточных полосах частоты; высокий динамический диапазон амплитуд обрабатываемых сигналов; высокая скорость обработки результирующих спектров входных сигналов; демодуляция AM, FM сигналов в реальном масштабе времени; полная компенсация фазовых сдвигов сигнала возбуждения в методе ВЧ навязывания; формирование напряжения смещения для активизации работы радиоэлектронных устройств; наличие автоматических режимов анализа; встроенные в основной блок компьютер с операционной системой Windows и 17" TFT дисплей.

Основные технические характеристики: обнаружение эффекта ВЧ навязывания в электронных устройствах и проводных линиях: диапазон частот сигнала возбуждения 10...100000 кГц; максимальный уровень сигнала возбуждения ±3 В; диапазон регулировки уровня сигнала возбуждения не менее 40 дБ; электронный аттенюатор входного сигнала 0,20 дБ; Чувствительность по входу (для модулирующего сигнала, при соотношении с/ш 10 дБ) не более 10 мкВ; шаг перестройки по частоте 0,1; 1; 10; 100 кГц; компенсация фазового сдвига между сигналом возбуждения и ответным сигналом ±90°; полосы пропускания для модулирующего сигнала 3, 25 кГц; обнаруживаемые виды модуляции — AM, FM, PM; центральные частоты октавных полос сигнала акустического возбуждения 250, 500, 1000, 2000, 4000, 8000 Гц; уровень звукового давления тестового акустического сигнала в полосе 150...10000 Гц не менее 90 дБ.

Анализ спектра входного сигнала: диапазон частот входного сигнала 10...100000 кГц; чувствительность по входу (при соотношении с/ш 10 дБ) не более 120 мкВ; входное сопротивление 100 Ом; электронный аттенюатор входного сигнала 0,20 дБ; виды подключения к входному разъему — симметричный, несимметричный; напряжение смещения 0, ±12 В; максимальная амплитуда входного сигнала ±10 В; разрешение по частоте (при количестве точек отсчета 1024) 0,03; 0,3; 3; 30 кГц; время формирования одиночной выборки спектра сигнала (при количества точек отсчета 1024) не более 0,1 с; полосы пропускания для преобразования сигнала (по уровню −3 дБ) 25; 250; 2500, 25000 кГц; полосы обзора результирующего спектра сигнала 50; 500; 5000; 50000; 100000 кГц; обнаруживаемые виды модуляции — AM, FM, PM; возможность демодуляции сигналов AM, FM, PM.

Анализ звуковых частот: диапазон частот входного сигнала 100... 25000 Гц; чувствительность по входу (при соотношении с/ш 10 дБ) не более 10 мкВ; динамический диапазон не менее 120 дБ; входное сопротивление 50 кОм; виды подключения к входному разъему — симметричный, несимметричный; напряжение смещения 0; ±12 В; максимальная амплитуда входного сигнала ±2 В; анализ спектра сигнала в полосе обзора 6; 50 кГц; мощность выходного усилителя 20 Вт.

Рис. 5.16. Анализатор проводных и телефонных линий TALAN

Цифровой анализатор проводных и телефонных линий TALAN (рис. 5.16) предназначен для анализа, проверки и тестирования проводных линий на наличие устройств негласного съема информации.

Цифровой анализатор проводных и телефонных линий TALAN в своем составе имеет: цифровой демодулятор для проверки любых телефонных линий на наличие несанкционированного звукового сигнала (позволяет демодулировать сигнал большинства АТС PBX/ACD, используемых в мире, возможность обновления типа АТС через компьютер); частотный рефлектометр для выявления подключения устройств негласного съема информации в проводных линиях; локатор нелинейностей с поисковым зондом для трассировки линии и локализации электронных устройств; осциллограф с активным входом (20 Гц...20 кГц); цифровой мультиметр для измерения параметров линии; автоматический коммутатор для тестирования всех комбинаций пар при подключении к многопроводной линии; широкополосный детектор радиочастотных сигналов для тестирования линий на наличии радиочастотных сигналов до 8 ГГц; генератор напряжения смещения ±80 В, прямое цифровое управление;

мультитестовая система для последовательного проведения тестов со всеми комбинациями пар линий, сохранение результатов в базе данных для последующего сравнения.

Выявление утечки информации в инфракрасном диапазоне. Рассматриваются два вида каналов утечки информации. Один из них создается за счет применения технических средств с передачей перехваченной информации в инфракрасном диапазоне. Другой основан на облучении стекол оконных проемов направленным лучом источника инфракрасных излучений и приеме отраженного сигнала промодулированного акустикой помещения. Для выявления обоих каналов утечки необходимо провести одинаковые подготовительные мероприятия. Необходимо правильно выбрать время проведения проверки, а именно время, когда в окна контролируемого помещения не попадают прямые солнечные лучи.

В проверяемом помещении необходимо выключить лампы накаливания и источники интенсивного теплового излучения. Целесообразно также выключить (если имеется) цветной телевизор, так как датчики приборов могут реагировать на «теплые» тона изображения.

Специфика инфракрасных закладочных устройств предопределяет необходимость обеспечения прямой видимости между передатчиком закладочного устройства и приемником инфракрасных излучений. Следовательно, излучение передатчика может быть только через оконные проемы. Поэтому поиск опасных сигналов рекомендуется начинать от окон помещения, передвигаясь вглубь его. Поскольку у передатчика может быть достаточно узкая диаграмма направленности, а угол зрения датчика прибора 30°, необходимо плавно изменять пространственную ориентацию датчика. Признаком наличия инфракрасного излучения при применении «Пираньи» является появление окрашенных сегментов шкалы индикатора уровня и щелчков звуковой индикации в режиме TONE после окрашивания 4-го элемента шкалы. Анализ обнаруженных сигналов может производиться «на слух» в режиме AUD, а также визуально с использованием встроенного осциллографа и анализатора спектра. Локализация источников инфракрасного излучения наиболее точно осуществляется сочетанием амплитудного метода и метода акустозавязки. Использование программно-аппаратного комплекса «Спектр-Professional» позволяет повысить вероятность выявления ЗУ, работающих в инфракрасном диапазоне.

Для выявления внешних потенциально опасных инфракрасных излучений необходимо обследовать каждый оконный проем. При этом датчик ориентируется в сторону окна. Плавно изменяя его пространственное положение, провести обследование всей площади оконного проема. Поскольку зондирующий сигнал не имеет модуляции,

то его наличие может быть оценено только по показаниям индикатора уровня и тональной индикации в режиме TONE для «Пираньи» и наличием сигналов облучения в диапазоне инфракрасного спектра на мониторе ПЭВМ для программно-аппаратного комплекса «Спектр-Professional».

Выявление утечки информации по низкочастотным магнитным полям. Данные каналы возникают при использовании по целевому предназначению (ПЭВМ, переговорных устройств, систем звукоусиления магнитофонов, телефонов и т. д.). Поэтому одной из основных задач следует считать исследование таких средств на наличие низкочастотного магнитного поля. Сопутствующими могут считаться задачи поиска скрытой (несанкционированно проложенной) проводки и обнаружения работающих диктофонов. По своим тактическим возможностям для реализации процедуры поиска низкочастотных магнитных полей из современных поисковых приборов наиболее подходят универсальные приборы типа «Пиранья». Особенности их применения сводятся к следующим положениям.

Перед поиском целесообразно выключить в помещении люминесцентные светильники, а антенну прибора включить в дифференциальном режиме (переключатель на корпусе антенны поставить в положение «к белой точке»). Потенциальные источники опасных низкочастотных магнитных полей следует проверять раздельно, включая их в работу поочередно.

При исследовании технических средств необходимо оценить дальность распространения магнитных полей и особенности их спектра. Для этого первоначально разместить магнитную антенну в непосредственной близости к исследуемому объекту. Зафиксировать по осциллограмме относительный уровень поля. Удаляясь от исследуемого средства и изменяя пространственную ориентацию антенны, оценить дальность уверенного приема низкочастотного сигнала.

Применительно к усилителям звуковой частоты, имеющим выходной трансформатор, следует оценить дальность уверенного (разборчивого) приёма речевого (тестового) сигнала. Такая оценка может послужить основой для правильного выбора мест установки соответствующих средств по отношению к наружной стороне помещения и варианта их совместного расположения в помещении. При необходимости включить режим SA, проанализировать спектрограмму и записать ее в энергонезависимую память.

Для поиска скрытой проводки необходимо последовательно обойти все стены помещения, располагая магнитную антенну в непосредственной близости к ним. Зафиксировать область возрастания уровня поля и, перемещая антенны по горизонтали и вертикали, определить прохождение трассы скрытой проводки.

Некоторые поисковые приборы обладают возможностью обнаружения работающих диктофонов. Реализации этой возможности определяется как уровнем магнитного поля, создаваемого их двигателями, так и уровнем магнитного фона помещения. Однако не всегда может быть достигнут положительный поисковый результат, особенно если расстояние между диктофоном и магнитной антенной прибора 30 см и более.

Для окончательного определения наличия (отсутствия) в обследуемом предмете ЗУ необходимо еще раз тщательно осмотреть с помощью луп с различными коэффициентами увеличения этот предмет или обследуемое место в элементе строительной конструкции, обращая внимание на возможное наличие в них отверстия, указывающего на наличие акустического канала утечки информации. После этого обследуемый предмет или обследуемое место проверить ещё раз металлоискателем и нелинейным локатором (НЛ) при различном расположении его относительно используемых приборов. Если снова металлоискатель и НЛ будет формировать прерывистый звуковой сигнал, указывающий на наличие в нем ЗУ, необходимо по возможности разобрать обследуемый предмет и убедиться в наличии (отсутствии) в нём ЗУ.

Эффективность использования в поисковых исследованиях металлоискателя и НЛ зависит от скорости перемещения их относительно обследуемого предмета (поверхности), которая не должна превышать 30 см/с в разных направлениях, и от удаления металлоискателя и антенны НЛ от обследуемого предмета (поверхности), которое не должна превышать 15 см.

При обнаружении объекта поиска совместно с руководством решается вопрос о дальнейшей судьбе ЗУ, которая может быть реализована по следующим направлениям:

- ЗУ изымается;
- ЗУ консервируется;
- ЗУ используется для дезинформации вероятного противника.

При принятии решения вопроса по изъятию из мест негласно установленного ЗУ осуществляется его изъятие и демонтаж таким образом, чтобы устройство осталось работоспособным, а место его размещения, по возможности, не отличалось от первоначального вида. После изъятия ЗУ производится измерение в лабораторных условиях его электрических характеристик, на основании которых уточняются следующие потребительские параметры найденного ЗУ:

- канал утечки информации (акустический, радио, телефонный, радиотелефонный, электросетевой и т. д.);
- метод внедрения ЗУ (заходный или беззаходный):

- вид негласно снимаемой информации (акустические сигналы, сигналы телефонных переговоров, паразитные излучения компьютеров и т. д.);
- способ негласного съема сигналов информации (индуктивный, ёмкостной, низкочастотный, высокочастотный, дистанционный и т. д.);
- вид источника питания (автономный, электросетевой);
- ресурс работы от автономного источника питания;
- ориентировочная дальность передачи сигналов информации (в пределах обследуемых помещений, до телефонного шкафа, до электросчетчика, в пределах нескольких помещений и т. д.);
- ориентировочное время внедрения ЗУ;
- технический и технологический уровень изготовления изделия.

Оценку по всем выше перечисленным потребительским параметрам могут произвести специалисты, имеющие большой опыт поисковых исследований и работы с радиотехническими средствами.

При принятии решения о консервации найденного ЗУ последующие работы могут проводиться по двум возможным вариантам.

По первому варианту ЗУ дорабатывается таким образом, чтобы оно оставалось работоспособным, но съем и передача сигналов информации не осуществлялась. Для ЗУ, использующего в качестве канала передачи сигналов информации акустический канал, это может быть достигнуто:

- во-первых, заклеиванием акустического отверстия липкой лентой, пластилином или другим материалом;
- во-вторых, разрывом связи устройства с каналом передачи сигналов. Для других обнаруженных ЗУ они дорабатываются таким образом, чтобы в результате по используемому им каналу утечки информации сигналы не передавались.

По второму варианту «консервируется» не ЗУ, а объект поиска так, чтобы в нем отсутствовали сигналы конфиденциальной информации т. е. в этих местах не производятся разговоры, переговоры и компьютерные расчёты, несущие конфиденциальную информацию. Следовательно, в этом случае по возможным каналам утечки информации передаются сигналы, не несущие никакой конфиденциальной информации.

При принятии руководством организации объекта поиска решения по использованию найденного ЗУ для дезинформации прогнозируемого противника, необходимо уточнить следующие его потребительские характеристики:

- используемый канал утечки информации;
- способ съема сигналов информации;

- вид источника питания ЗУ (автономный, электросетевой или телефонный);
- ресурс работы ЗУ и передачи сигналов информации при автономном питании;
- дальность передачи сигналов информации.

После этого необходимо проверить функционирование ЗУ. Следует отметить, что для подтверждения передачи дезинформационных сведений прогнозируемому противнику необходимо:

- во-первых, создать тракт передачи-приёма сигналов информации, используя в качестве передатчика найденное ЗУ, а в качестве приёмника сигналов информации целесообразно использовать приёмник с параметрами, аналогичными приёмнику, используемому прогнозируемым противником;
- во-вторых, помочь руководству объекта поиска в разработке сценария дезинформационной среды, который должен иметь обратную связь с предпринимаемыми действиями прогнозируемого противника. Такой алгоритм функционирования системы и сценария её использования позволит подтвердить или опровергнуть прогнозируемого противника и выяснить его замыслы.

После окончания дезинформационной игры по решению руководства объекта поиска ЗУ может быть снято или законсервировано. Процедура изъятия или консервации выполняется таким же образом, как и ранее описанная. По окончании осмотра и проверки предметов быта и интерьера на наличие в них ЗУ они должны быть установлены на прежнее место.

Выявление неработающих во время проверки ЗУ. Основным средством обнаружения неработающих специальных устройств съёма информации при проведении проверок является нелинейный локатор. В основу работы НЛ заложен принцип обнаружения отраженного сигнала зондирования от предметов, имеющих в своем составе полупроводниковые элементы, независимо от их состояния на второй гармонике зондирующего сигнала. Для эффективного использования прибора необходимо точно определить особенности среды установки и характера расположения ЗУ в этой среде.

Основной обнаружительный признак, на который реагирует НЛ, зто наличие в ЗУ p-n-перехода, что является обязательным составным элементом любой электронной схемы.

Однако в некоторых случаях прибор не может с достаточной степенью вероятности обнаружить этот признак, а именно когда:

- ЗУ установлено в корпусе, надежно изолирующем электронику от воздействий зондирующего сигнала. Примером таких ЗУ являются некоторые типы цифровых диктофонов в экранированных

корпусах и радиозакладки, имеющие фильтрацию по антенному входу с экранированным корпусом;

- ЗУ установлено в электронное средство, размещенное в проверяемом помещении (например, радиозакладка в элементе питания кварцевых часов). НЛ в данном случае применять практически невозможно. Других способов обнаружения этих средств несколько, например визуальный осмотр, рентгенография, сравнение с проверенным аналогом, контроль изменения различных физических параметров;
- ЗУ установлено в железобетонной стене за сеткой-рабицей (например, установка электронного стетоскопа). Выявление таких средств весьма сложно, так как НЛ получает смесь сигналов закладки и коррозийности сетки-рабицы;
- ЗУ установлено за массивной металлической конструкцией (например, балкой), когда зондирующий сигнал НЛ может отразиться от нее и не дойти до закладки. Применение металлодетектора покажет наличие металла. Объект идентифицируется как балка. Добавьте к этому невозможность использования рентгена во многих случаях (например, наружная стена) или балка окажется достаточно толстой и пропуск гарантирован. Способы выявления — контроль за строительством объекта, постоянный мониторинг возможных ТКУИ;
- отсутствие в ЗУ, расположенном в проверяемом помещении, электронной составляющей, расположенной в зоне действия НЛ (например, микрофон типа COM, звуковод, на удаленном окончании которого расположен микрофон с усилителем). Способы обнаружения — тщательный визуальный осмотр проверяемого помещения.

Прежде чем рассматривать вопрос о тактике выявления неработающих электронных устройств негласного получения информации, остановимся на методике выбора НЛ.

В настоящее время на рынке очень много предложений НЛ. Рассмотрим основные особенности выбора НЛ.

Прежде всего при выборе необходимо обратить внимание на частоту работы НЛ. Выделенный для работы НЛ диапазон частот соответствует частотам работы GSM. Не углубляясь в размышления о преимуществах работы на той или иной частоте, необходимо отметить, что зачастую возможно наличие в наушниках сигналов стандарта GSM, который при длительной работе оказывает сильное мешающее воздействие. Таким образом, выбранный прибор должен позволять отстраиваться от этих помех. Так как процесс поиска ЗУ с помощью НЛ достаточно продолжителен, необходимо обратить внимание на эргономические характеристики прибора, связанные прежде всего

с удобством в работе. Для наиболее эффективного поиска необходимо, чтобы НЛ имел возможность принимать отраженный сигнал на второй и третьей гармонике от зондирующего сигнала. Желательно иметь возможность прослушивания акустического отклика и режим 20K. При выборе необходимо также учитывать длительность работы НЛ от автономного источника питания.

При рассмотрении тактики работы с НЛ остановимся на основных принципах поиска ЗУ. Есть несколько подходов к тактике применения НЛ. Наиболее подробно остановимся на одном из них.

При начале поиска НЛ настраивается на максимальную мощность излучения, позволяющую выполнять поиск с наибольшей скоростью. Антенная система НЛ спиралеобразно перемещается по проверяемой поверхности. При этом возможны различные варианты перемещения, которые должны обеспечить гарантированный контроль всей проверяемой поверхности.

При обнаружении подозрительного отклика для точного определения местоположения объекта используется метод постепенного уменьшения мощности и чувствительности НЛ. Поймав отклик, необходимо, плавно перемещая антенну, получить максимум уровня принимаемого сигнала. После этого уменьшить мощность НЛ. При уменьшенной мощности необходимо уточнить местоположение объекта, дающего отклик, по максимальному уровню принимаемого сигнала. В некоторых случаях возможно определение его местонахождения с точностью до 2...5 см, что вполне достаточно для последующего визуального обнаружения объекта.

После получения отклика от объекта необходимо принять решение, к какому из видов относится принятый сигнал. Особенности современных НЛ заключаются в том, что информация воспринимается из двух источников — на слух (из наушников) и визуально (две шкалы с уровнем сигналов на второй и третьих гармониках). Если в наушниках прослушивается чистый тональный сигнал и на шкале видно сильное превышение сигнала второй гармоники над третьей, то объект идентифицируется как p-n-переход. При этом включение режима 20K или выключенная модуляция позволяет в случае работы ЗУ услышать её характерные признаки. Особенно хочется отметить качество этого способа у режима с выключенной модуляцией. Радиозакладка с открытым каналом передачи информации слышна не хуже, чем на обычном приемнике. Но независимо от того, есть в этом режиме сигнал или нет, оператор обязан изъять объект и идентифицировать его. Это связано с тем, что закладка может быть выключена или у нее разрядился элемент питания. Возможно отсутствие в изделии аналогового сигнала.

При поверке больших площадей рекомендуется предварительно начертить на листах план стен, потолка, пола, разбив схему на квадраты (например, 50×50 см). Обнаружив отклик, отметьте на листе точку, где он наблюдался. Рекомендуется также отмечать обнаруженные подозрительные места непосредственно на объекте поиска, используя для этого подручные средства, не портящие проверяемые объекты.

После обследования всего помещения необходимо идентифицировать обнаруженные отклики. Это связано с тем, что постоянные отвлечения для идентификации и визуального обследования объекта быстро утомляют оператора (если он работает один), а утомляемость ведет к ухудшению внимания и, следовательно, к возможному пропуску подозрительного отклика.

Наиболее сложным является поиск с помощью НЛ в сильной помеховой обстановке. Большое количество проводников, металлических изделий могут привести к обнаружению МОМ-диода (металл–окисел–металл). Как их отличить от p-n-перехода? Если при простукивании в районе объекта наблюдается треск, то обнаружен МОМ-диод (например, ключи, скрепки или монеты, положенные одни на другие). Для более качественного получения отклика рекомендуется использовать резиновый молоток. Иногда после удара молотком МОМ-диод разрушается и сигнал пропадает. Например, часто в местах пересечения направляющих подвесных потолков происходит образование МОМ-диода. Достаточно легкого удара, чтобы его разрушить.

Еще одной сложностью при работе с НЛ является наличие в помещении электронных средств. В некоторых случаях нет возможности вынести из помещения электронное оборудование, и его переносят из угла в угол. В таких условиях может появиться так называемый «призрак». При наведении антенны на стену получаете четкий отклик, который идентифицируется по всем признакам как p-n-переход. Для окончательного вывода о наличии ЗУ направьте антенну НЛ на обнаруженный объект под другим углом. Если сигнала нет, то возможной причиной его появления может стать компьютер, стоящий позади в нескольких метрах. Хотя все НЛ имеют направленные антенны, у них существует задний лепесток диаграммы направленности. Он небольшой, но есть у всех НЛ. В некоторых случаях происходит захват электронных средств, расположенных в четырех метрах сзади объекта поиска. После перемещения оборудования в другое место и пропадании сигнала можно сделать вывод, что это ложный сигнал, т. е. НЛ принимал сигнал, полученный из-за наличия обратного лепестка диаграммы направленности. Контроль отклика под разными

углами относительно поверхности обследования эффективен при определении местоположения объекта, например, за стеной. Направив антенну на объект с двух разных точек, можно определить, находится он непосредственно за стеной или на удалении.

Возможно получение сигнала отклика от НЛ при наводке зондирующего сигнала на проводные линии, в окончании которых находится электронные средства. Например, можно поймать ретранслятор или телевизор, в который вставлена антенна и сигнал котрого наводится по коаксиальному кабелю. Достаточно выдернуть проводник из электронного устройства, и сигнал пропадет.

Если у поисковой бригады есть время и возможность, то необходимо визуально оценить подозрительные места, обнаруженные в процессе осмотра с помощью НЛ: поднять подвесные потолки, разобрать розетки, проверить вентиляционные каналы, проверить металлодетектором изделия на содержания металла и т. д. При этом необходимо правильно оценивать объект проверки. Например, маловероятно наличие ЗУ в бетонной стене. При отсутствии на ней видимых следов вскрытия и попытки их камуфлирования и в ряде случаев (при дефиците времени) такое место не подвергается проверке.

Второй метод работы с НЛ связан с другим подходом к методике работ. Поисковые работы с НЛ начинают с медленного сканирования антенной любой проверяемой поверхности в зоне поиска при отключенном излучении. Оператор буквально «красит» каждую поверхность, включая стены, пол, потолок, оборудование. Эта процедура предназначена для обнаружения генерирующих электромагнитные поля приборов и поглощает много времени — обычно она протекает со скоростью 0,2...0,4 м^2/мин.

Далее уже при включенном облучающем сигнале антенной сканируют стены и остальные поверхности на расстоянии от них по крайней мере 2...3 м, это позволяет обнаружить и изолировать предметы, создающие помехи. После очистки зоны поиска от этих предметов расстояние до НЛ сокращается до 1...1,5 м и процедура повторяется. В дальнейшем расстояние сокращается до 0,5 м или непосредственного контакта с объектом и проводится несколько операций проверки при постепенном повышении мощности излучения НЛ от минимально возможного уровня до максимального уровня зондирующего сигнала. Сканирование плоских поверхностей происходит со скоростью 0,03 м^2/с, сложных — с еще меньшей. В результате для проверки небольшого офиса (менее 20 м^2) необходимо 2...3 ч, офиса среднего размера — 3...4 ч, а для более крупных учреждений — 6...8 ч или даже несколько дней.

Обнаруженные нелинейным локатором подозрительные места подвергают рентгеноскопическому анализу. При этом нужно помнить,

что каждые 10 кВ напряжения на трубке излучателя позволяют просветить около 1 см толщины материала.

Таким образом, методика применения НЛ для выявления ЗУ прежде всего зависит от характера проверяемого объекта и стоящих перед проверяющими целей.

Практика проведения поисковых работ позволяет сделать вывод, что внедрение средств съема в ограждающие конструкции требует благоприятных условий и профессиональной подготовки. Гораздо проще установить подслушивающее устройство, не заходя в помещение, с внешней стороны ограждающих поверхностей. Балки, трубы, стены и другие несущие конструкции здания хорошо проводят звуковые волны на десятки метров, поэтому стетоскопы могут быть установлены достаточно далеко от проверяемого помещения. Возможность существования такого канала утечки проверяют измерительным электронным стетоскопом.

Поиск устройств негласного съёма информации, внедрённых в электронные приборы. Поиск ЗУ в электронных приборах (телефонных аппаратах, телевизорах, ксероксах, радиоприёмниках, компьютерах и т. д.) на объектах поиска целесообразно осуществлять в следующей последовательности:

- проводится зрительная фиксация мест размещения всех электронных приборов на объекте поиска;
- затем проводится анализ электромагнитного поля обследуемых электронных приборов как в работающем, так и в не работающем состояниях, позволяющий выявить и локализовать место размещения ЗУ.

С целью оперативного обнаружения радиоподслушивающих устройств в электронных приборах по электромагнитному полю целесообразно использовать обнаружители поля, позволяющие не только зафиксировать ЗУ, но и локализовать место их размещения независимо от используемого вида модуляции, диапазона частот и излучаемой мощности.

Принцип действия электромагнитных индикаторов поля основан на широкополосном детектировании электрического (электромагнитного) поля и формирования сигнала тревоги при приближении его антенны к электронному прибору, в котором размещается работающее радиоподслушивающее ЗУ.

Радиус обнаружения такого ЗУ зависит от излучаемой им мощности и для всех известных индикаторов поля не превышает одного метра при мощности излучения более 5 мВт.

Следует отметить, что многие современные индикаторы и поля имеют акустическую обратную связь, проявляющуюся в виде акустической завязки. Акустическая завязка сводит к минимуму возможных

ложных срабатываний и позволяет идентифицировать радиоподслушивающие ЗУ по тональному звуковому сигналу, уровень которого увеличивается при приближении к работающему устройству.

Наряду с этим ряд индикаторов поля выполняет не только функции обнаружения и локализацию мест размещения радио подслушивающих ЗУ, но и ряд других функций.

Во всех известных индикаторах поля имеется аттенюатор, обеспечивающий ослабление входного электромагнитного сигнала, что позволяет упростить процесс поиска подслушивающих ЗУ в условиях сложной электромагнитной обстановки, имеющей место на объекте поиска.

Поиск радио- и радиотелефонных подслушивающих ЗУ, в электронных приборах осуществляется как во включённом, так и выключенном состояниях.

Следует иметь в виду, что для обеспечения надёжного поиска радио- и радиотелефонных подслушивающих ЗУ в электронных приборах с использованием индикатора поля необходимо, чтобы исследуемый электронный прибор был размещён по возможности в определённом месте так, чтобы он находился от других приборов на расстоянии более одного метра. Такое размещение исследуемого электронного прибора исключит влияние на процесс обнаружения радиопередающих устройств, имеющихся в других приборах.

Перед началом поиска необходимо, по возможности, все электронные приборы выключить, выдвинуть антенну индикатора поля на два колена и включить его. После этого, медленно перемещая антенну во всех возможных направлениях вдоль анализируемого электронного прибора, производится обследование всех электронных приборов, находящихся на объекте поиска.

Если при приближении антенны индикатора поля к исследуемому электронному прибору он формирует сигнал тревоги в виде акустического сигнала характерного для объекта поиска и изменяющегося при резких хлопках и стуках, а уровень его увеличивается при приближении индикатора поля к испытываемому электронному прибору и наоборот уменьшается при удалении, то это указывает на то, что в нём возможно размещено радиоподслушивающее ЗУ. При этом, если сигнал обусловлен работой акустического радиоподслушивающего ЗУ, на выходе индикатора поля будут прослушиваться признаки акустического сигнала объекта поиска, а при наличии в электронном приборе работающего радиотелефонного подслушивающего ЗУ будут прослушиваться признаки телефонных переговоров.

Следует обратить внимание, что при большом уровне акустического сигнала в головных телефонах индикатора поля его можно уменьшить или потенциометром индикатора поля, или уменьшением дли-

ны его телескопической антенны. В процессе анализа электронных приборов индикатор поля может сформировать ложный сигнал, который обусловлен наличием электромагнитного поля от вещательной или телевизионной станции. Особенностью этого ложного акустического сигнала, обусловленного работой вещательной или телевизионной станцией, является наличие в нём признаков музыкальной или речевой передачи, не характерных для объекта поиска, либо признаков характерного «рокота», обусловленного детектированием строчной развёртки телевизионного сигнала.

Такой алгоритм поиска ЗУ в электронных приборах с использованием индикатора поля необходимо осуществить при включённом и выключенном состояниях каждого анализируемого электронного прибора. При этом остальные электронные приборы должны находиться в выключенном состоянии.

При подтверждении того, что источником электромагнитного излучения является исследуемый электронный прибор, переходят к визуальному осмотру прибора и, по возможности, к его разборке. Для этих целей необходимо иметь различные инструменты, лупы с различными коэффициентами увеличения, приспособления, полный набор которых имеется в поисковом комплекте Parat.

Анализируемый электронный прибор вскрывают. Затем тщательно визуально и с помощью луп осматривают все радиоэлементы и печатные платы. При этом особое внимание обращается на возможное наличие в них дополнительных плат или радиоэлементов, на изменения в штатных печатных платах, просматривая номиналы и размеры радиоэлементов и наличия в них отличительных признаков. Причём особое внимание должно быть уделено конденсаторам ёмкостью свыше 20 мкФ, поскольку в них могут быть размещены радиоэлементы радио-, радиотелефонных или телефонных подслушивающих ЗУ. Отличительным признаком таких конденсаторов является наличие у них, как правило, со стороны выводов акустического отверстия диаметром 0,3...1 мм.

Если в процессе визуального осмотра не найдены радиоэлементы ЗУ, далее осуществляют их поиск по характерным признакам, формируемым в процессе монтажа. Необходимо иметь в виду, что если монтаж электронного прибора выполнен в заводских условиях, пайки, как правило, имеют одинаковую площадь и высоту и практически не имеют заусенцев, а печатные платы покрыты светлым лаком и на их поверхностях отсутствует канифоль. Наличие нарушения лакового покрытия желтизны свидетельствует о возможно внедренных радиоэлементах ЗУ. Для проверки наличия в пайках заусенцев необходимо провести ладонью по печатной плате. В тех местах, где были осуществлены дополнительные пайки, будут ощущаться острые заусенцы.

Чтобы окончательного убедиться в наличии (отсутствии) в исследуемом приборе радиоэлементов ЗУ, необходимо произвести сравнение их расположения с монтажной схемой (если такая имеется), копией платы или с фотографией расположения радиоэлементов на плате аналогичного изделия. Если отличительных признаков по монтажным платам нет, необходимо повторить оценку наличия электромагнитного излучения в разобранном исследуемом электронном приборе. По вышеописанной методике проверяется наличие электромагнитного излучения при включенном и выключенном приборе. При повторном подтверждении наличия электромагнитного излучения, которое может принадлежать ЗУ, анализируемый электронный прибор ещё раз разбирают и тщательно проводят визуальный и приборный осмотр и окончательно убеждаются в наличии (отсутствии) ЗУ.

При обнаружении в анализируемом электронном приборе подслушивающего устройства необходимо, по возможности, восстановить его функционирование в разобранном электронном приборе, после чего необходимо сообщить руководителю организации объекта поиска о найденном устройстве и доказательно показать его наличие, в том числе, если это возможно, показать его функционирование. Затем совместно с руководителем объекта поиска решить вопрос по изъятию (не изъятию) подслушивающего устройства из анализируемого электронного прибора.

Примечание: акустический фон для активизации радиозакладок создается размещением в контролируемом помещении тестового источника звука. В качестве такого источника можно использовать магнитофон с хорошо известной музыкальной или речевой фонограммой. Не рекомендуется использовать в этих целях радиоприемник или телевизор, так как создаваемый ими звуковой сигнал, переизлучаемый радиозакладкой, может совпасть с радиосигналом выбранной вещательной станции. Выбор громкости тестового звукового сигнал определяется размещением источника тестового сигнала, расположением проверяемого прибора и чувствительностью микрофона радиозакладки.

Микрофонами могут являться звонок телефона, шаговый двигатель электрочасов и т. д. Устройства, у которых обнаружены паразитные, возникающие за счет конструктивных дефектов информативные излучения, по возможности заменяют или удаляют из помещения при проведении ответственных переговоров.

После проверки электроприборы опечатывают специальными пломбами или маркируют ультрафиолетовыми метками.

5.1.3. Заключительный этап проверки

Работы данного этапа, хотя и проводятся без применения каких бы то ни было технических средств, тем не менее, по своей важности

не уступают предыдущим этапам. Цель данного этапа в доступной и убедительной форме представить руководителю проверяемой организации необходимые отчетные материалы по результатам проведенной работы. Для качественного и полного выполнения работ данного этапа целесообразно придерживаться следующего алгоритма:

- обработка результатов проверки и оформление протоколов (протоколы с указанием мест срабатывания исследовательских приборов, участков вскрытий ограждающих поверхностей, описанием подозрительных предметов мебели и интерьера; протоколы изъятия средств съема информации и т. д.);
- анализ технических характеристик и свойств обнаруженных и изъятых ЗУ;
- описание проведенных работ с основными характеристиками и полученными результатами;
- заключение о степени защищенности объекта от несанкционированного съема информации;
- рекомендации по устранению и нейтрализации технических каналов утечки конфиденциальных сведений;
- составление акта проведения комплексной специальной проверки;
- утверждение отчетных итоговых документов руководителем предприятия.

Более детально рассмотрим особенности выполнения работ данного этапа.

Обработка результатов проверки и оформление протоколов. Перед выполнением работ по обработке результатов проверки необходимо собрать и систематизировать полученные в ходе проведения проверки материалы, которые могут понадобиться для отработки отчетных материалов. В перечень этих документов могут входить: записи выполняемые специалистами в ходе проведения проверки, текущие отчетные материалы по работе с тем или иным оборудованием, схемы, таблицы, данные радиомониторинга и т. д.

Затем проводятся работы, связанные с уточнением документов, характеризующих объекты проведения поисковых работ:

- уточняются и корректируются записи в регистрационных журналах учета мебели, оборудования, уточняются и вновь заносятся места расположения скрытых меток с соответствующими пояснениями и схемами размещения, фиксируются поставленные пломбы и печати;
- уточняются планы проверенных помещений и, при необходимости, вносятся изменения в схемы размещения предметов, мебели, наличия новых элементов, не зарегистрированных в межпроверочный период;

- отрабатываются материалы по обнаруженным средствам несанкционированного съёма информации, описание характеристик ЗУ, схемы их размещения, способы и время, необходимое на установку, ориентировочное время установки;
- отчет по радиомониторингу с соответствующими выводами и другие необходимые материалы.

В ходе этого этапа целесообразно обобщить опыт, полученный в ходе проведения поисковых работ и сопутствующих им исследований. Это позволит выявить недостатки в используемых методиках и применяемых приборах, оценить реальность и правдоподобность и эффективность использованных легенд для прикрытия поисковых мероприятий и активизации ЗУ. Результаты проведенного анализа позволять разработать более совершенные методы использования аппаратуры и возможно приведут к новым решениям. Анализ результатов радиомониторинга позволит пополнить базу данных характеристиками новых средств, применённых противником.

Анализ технических характеристик и свойств обнаруженных и изъятых ЗУ. Рассматривая данный вопрос, необходимо прежде всего обратить внимание на то, что применение средств несанкционированного съема информации в России разрешено только структурам, имеющим разрешение на проведение оперативно-розыскной деятельности. Применение ЗУ требует получения этими структурами разрешения от судебных органов. Следовательно, обнаруженные устройства рекомендуется сдать в ФСБ для избежания неприятностей при их случайном обнаружении этими органами, тем более что применять и, тем более, сбывать эти средства законом запрещено и может привести к уголовной ответственности.

Однако с целью подготовки специалистов по выявлению этих средств необходимо знать их потребительские характеристики, особенности применения, общий вид и т. д. Необходимо учитывать еще один аспект, касающийся неизбежного отчета перед руководством о результатах проверки: для грамотного ответа на вопросы руководителя необходимо знать параметры и особенности функционирования обнаруженных ЗУ.

Особое внимание необходимо уделить ранее не применявшимся ЗУ с целью определения способов перехвата и передачи информации, выяснить методы закрытия канала передачи, особенности маскировки, время работы, наличие канала управления, какими средствами и с какого расстояния можно обнаружить, вид в векторной форме и спектральные характеристики, возможности по накоплению информации и передачи её в импульсе и т. д.

По результатам исследования целесообразно подготовить подробную справку, в которой необходимо отметить следующую инфор-

мацию: какого рода и откуда получало данное ЗУ, в каком состоянии оно находилось на момент обнаружения, ориентировочное время установки, особенности функционирования, метод передачи информации, возможная протяженность канала передачи и т. д.

Для получения ответов на эти вопросы обычно не требуется строгих инструментальных исследований. Существует достаточно много признаков, позволяющих при внешнем осмотре места установки ЗУ, самого устройства, а также в результате анализа его сигналов с помощью поисковой аппаратуры оценить возможные значения характеристик устройства. Ориентируясь на характеристики известных радиомикрофонов и сетевых микрофонов [116], можно с высокой степенью достоверности определить радиус съёма акустической информации таким устройством.

Подключение устройств к проводной линии говорит о возможном получением информации с линии и (или) возможном использовании линии в качестве источника питания. По типу или габаритам автономного источника питания можно судить о его ёмкости, а измерив ток потребления ЗУ, можно рассчитать возможную продолжительность непрерывной работы устройства. По относительному уровню сигнала и значению его несущей частоты можно судить о возможной дальности его распространения. Давность установки средства ЗУ в случае его питания от автономного источника можно оценить по степени разряда источника питания.

При невозможности провести прямые измерения характеристик найденного устройства можно попытаться провести его идентификацию с описанными в специальной литературе ЗУ [116]. Основными идентификационными признаками может быть внешний вид и назначение устройства (вид снимаемой информации), его массогабаритные характеристики, параметры энергопотребления и другие параметры устройства. Результаты этих работ должны пополнить базу данных по ЗУ.

Составление описания проведённых работ. Как правило, в число отчётных документов целесообразно включить описание проведённых поисковых и исследовательских работ с приложением поясняющих схем, рисунков, протоколов измерений, необходимых инженерно-технических выкладок. Если план проведения комплексной специальной проверки был разработан достаточно подробно и тщательно, то это не вызывает трудностей. Объём, как и необходимость составления этого документа, целесообразно заранее согласовать с руководством предприятия.

При составлении этого документа можно придерживаться следующей структуры.

В вводную часть целесообразно включить целевую установку, масштаб и время проведения проверки, перечень и краткую характеристику проверенных помещений, численный состав поисковой бригады, перечень использованных в ходе проверки приборов и оборудования.

В основной части описываются отдельно для каждого помещения следующие вопросы: перечень проведённых поисковых и исследовательских работ с указанием данных, отражающих трудозатраты на их проведение (площадь обследованных элементов ограждающих конструкций, количество и степень сложности проверенных предметов обстановки, длина проверенных коммуникаций и т. д.); описание каждой работы с указанием заводских номеров и даты последних поверок аппаратуры, использованной для проведения измерений, методики проведения измерений; результаты (протоколы) измерений и работы в целом (уровни сигналов, их частоты и другие параметры, обнаружено ЗУ или нет, выявленные каналы возможной утечки защищаемой информации); план помещения с указанием мест размещения аппаратуры, обнаруженных ЗУ и технических каналов утечки защищаемой информации.

Целесообразно включить в состав описания работ в качестве приложений протоколы измерений и отчётов, сформированные в результате работ с программно-аппаратными комплексами радиомониторинга.

Разработка рекомендаций по повышению защищённости помещений. Для руководства предприятия, кроме результатов поиска ЗУ, представляют и рекомендации по повышению защищённости проверенных помещений и предотвращению съёма защищаемой информации по выявленным потенциальным техническим каналам утечки. Исходя из объёма и степени детализации, эти рекомендации могут отрабатываться как отдельный отчётный документ, который может включать:

- описание выявленных потенциальных ТКУИ для каждого проверенного помещения со схемами и краткими пояснениями (легендами);
- оценку вероятности использования противником потенциальных ТКУИ и степень защищённости каждого помещения от негласного съёма информации по выявленным потенциальным ТКУИ;
- конкретные рекомендации по мерам и способам предотвращения съёма защищаемой информации по выявленным каналам утечки и повышению защищённости помещений по каждому ТКУИ;
- рекомендации по организационным и режимным мерам, по изменению элементов конструкции помещений, инженерно-технических коммуникаций, рекомендации по установке специальных при-

боров и систем защиты, в том числе комплексных систем защиты помещений от утечки информации по техническим каналам, и другим техническим мерам повышения защищённости помещений;
- сводный перечень технических средств и систем защиты информации, рекомендуемых к установке на предприятии для повышения защищённости помещений;
- предложения по практическому использованию рекомендуемых технических средств и систем и объединению их в единую комплексную систему защиты информации.

Учитывая то, что потенциальные ТКУИ отличаются от реальных только временным отсутствием в своём составе средств разведки противника, перечень выявленных потенциальных ТКУИ обычно состоит из естественных каналов.

В отличие от искусственно созданных, естественные ТКУИ не обеспечивают комфортных условий приёма перехваченной информации, но существуют постоянно и могут быть использованы противником в любой момент. При этом количественная оценка потенциальных ТКУИ требует специальных измерений и исследований, которые должны проводиться по особым методикам, как правило, не включаемым в число работ по комплексной специальной проверке помещений. Однако руководство предприятия обычно ожидает от поисковиков хотя бы качественной оценки степени защищённости помещений от утечки информации.

Поэтому целесообразно заранее, ещё на этапе подготовительных работ, выяснить у руководства предприятия, нужны ли ему дорогостоящие специальные исследования для получения точных количественных оценок защищённости помещений или можно ограничиться качественными критериями. Как правило, достаточно знать, имеются ли в помещении незакрытые потенциальные технические каналы утечки информации и может ли потенциальный противник воспользоваться этими каналами для съёма информации. Однако зачастую приходится ограничиваться указанием зон энергетической доступности источников информативных сигналов, ранжированием выявленных каналов утечки информации по степени угроз, экспертными оценками вероятности съёма информации различными видами специальных технических средств и другими аналогичными показателями.

Общая оценка возможности утечки защищаемой информации через потенциальные ТКУИ может быть получена в результате анализа сведений о конструктивных особенностях здания и помещений, визуального осмотра проверяемых и смежных с ними помещений и проверки наличия информативных сигналов на границах возможного съема

информации с потенциальных технических каналов утечки, доступных противнику (контролируемой зоны).

Приборы поиска сигналов в проводных линиях позволяют оценить возможность съёма информации противником за счёт микрофонного эффекта и наводок. Комплекс обнаружения радиоизлучающих средств и радиомониторинга даёт возможность сравнить уровни информативных ПЭМИ средств оргтехники с уровнями известных источников излучения.

Документ целесообразно завершить предложениями по практическому использованию средств и систем защиты информации, рекомендуемых к установке, и объединению или внедрению рекомендуемых технических средств и систем в единую комплексную систему защиты информации в организации. В предложениях по практическому использованию средств и систем защиты можно указать:

- в каком временном режиме целесообразно использовать средства защиты (кратковременно, постоянно или периодически);
- кем должно приниматься решение на их применение;
- комплексно или по отдельности их лучше применять;
- как контролировать их работоспособность и эффективность;
- целесообразно ли вводить централизованное управление работой средств защиты и контроля и т. п.

Как правило, интеграция отдельных средств и систем защиты информации в единую комплексную систему даёт заметный выигрыш в качестве защиты информации. При этом расходы на защиту информации если и увеличиваются, то незначительно. Повышение эффективности защиты информации происходит, главным образом, за счёт централизованного управления ресурсами системы, повышения качества контроля за работой составляющих её технических средств, возможности быстрого реагирования на возникновение новых угроз утечки информации.

Составление акта проведения комплексной специальной проверки помещений. Основным итоговым документом, завершающим работы по обследованию помещений на наличие средств НСИ, является *акт проведения проверки.* Этот документ обычно включает:

- время проведения обследования;
- состав поисковой бригады;
- перечень обследованных помещений и объектов;
- перечень и объём основных поисковых работ и сопутствующих исследований;
- перечень использовавшейся поисковой и исследовательской аппаратуры;
- результаты проверки;

- где были обнаружены средства НСИ, их состояние и краткие характеристики;
- принятые по отношению к обнаруженным средствам меры (изъятие, нейтрализация, консервация с целью последующей дезинформации);
- выводы из оценки степени защищённости помещений и объектов отутечки защищаемой информации по различным каналам;
- рекомендации по повышению защищённости помещений и объектов и предотвращению утечки информации по выявленным техническим каналам её утечки.

Акт обычно подписывается руководителем и членами поисковой бригады, согласовывается с руководителем организации, проводившей поисковые работы, после чего предоставляется для утверждения руководителю предприятия (фирмы) или начальнику его службы безопасности.

Завершающие работы заключительного этапа. К завершающим работам этого этапа целесообразно отнести оформление итоговых и отчётных документов, подготовку к заключительной встрече с руководством предприятия и представление руководству предприятия разработанных по результатам проверки документов для утверждения.

Оформление документов по результатам проверки заключается в изготовлении необходимого числа экземпляров текстуальных и графических документов, их строгом учёте в соответствии с принятой системой регистрации и учёта документов, содержащих информацию конфиденциального характера, в подписании документов руководителем и членами поисковой бригады и согласовании содержания документов с руководством организации, проводившей проверку помещений. В случае проверки помещений силами сторонней организации в число документов, подготавливаемых для передачи руководству предприятия, включаются также учётные и регистрационные журналы.

Опыт проведения комплексных специальных проверок помещений позволяет сделать вывод о том, что представление подписанных и согласованных документов для утверждения руководству предприятия обычно выливается в беседу по вопросам защиты информации. Поэтому специалистам рекомендуется тщательно подготовиться к заключительной встрече, чтобы убедительно доказать обоснованность и необходимость выполнения рекомендаций по повышению защищённости помещений от утечки информации. Следует быть готовым к ответам на вопросы не только по поводу эффективности того или иного рекомендованного способа или средства защиты, но и к обоснованию затрат, необходимых для реализации каждой рекомендации. Поэтому целесообразно заранее подготовить каталоги современных технических средств и систем защиты информации, необходимые справки и

выкладки, прайс-листы фирм и организаций, занимающих в этой области ведущие позиции.

В ходе встречи с руководством для утверждения итоговых и отчётных документов рекомендуется раскрыть структуру документов, устно пояснить содержание отдельных пунктов, всесторонне обосновать содержащиеся рекомендации, обсудить вопрос о сроках проведения следующей проверки помещений. Целесообразно подчеркнуть, что успешное проведение «зачистки» помещений не должно успокаивать руководство, поскольку очередная атака на его секреты может начаться в любое время.

Пользуясь удобной возможностью довести до руководителя современные взгляды на систему информационной безопасности предприятия, можно в тактичной форме указать на необходимость ведения постоянного, а не периодического радиомониторинга важных служебных помещений. Это обусловлено всё возрастающим распространением дистанционно включаемых радиоизлучающих ЗУ, а также высокой вероятностью и простотой подброса радиомикрофонов в любое удобное для противника время. Радиомикрофон, например, может быть скрытно занесён и включён во время переговоров кем-то из его участников. Следует также указать, что только ведение круглосуточного непрерывного радиомониторинга позволяет надёжно выявить радиоизлучающие ЗУ с промежуточным накоплением информации и использующие для передачи информации в сжатом виде режим быстродействия.

Высока вероятность внедрения противником ЗУ в ПЭВМ или другие электронные приборы, особенно во время их ремонта или профилактического осмотра. В то же время выявление таких средств — довольно сложная задача. Целесообразно напомнить, что в важных служебных помещениях рекомендуется размещать только сертифицированные технические средства, прошедшие предварительный визуальный осмотр и специальную проверку. При этом подчеркнуть, что такую процедуру должны проходить не только новые электронные приборы, но и любые новые предметы и подарки, включая книги, фоторамки, авторучки, зажигалки и т. п.

В заключение встречи можно указать, что средства и методы негласного съёма информации постоянно совершенствуются, поэтому организационные и технические решения, сегодня эффективно препятствующие утечке конфиденциальной информации, могут в скором времени оказаться недостаточными. В этой связи созданная на предприятии служба безопасности и техническая система информационной безопасности должны развиваться с темпами, по крайней мере, не отстающими от нарастания угроз.

Следует помнить, что принятие решения по разработанным рекомендациям и всем обсуждавшимся вопросам остаётся за руководителем предприятия, поэтому изложение рекомендаций должно вестись в убедительной, но ненавязчивой и тактичной форме. Если в ходе этой встречи удастся достичь взаимопонимания, можно быть уверенным, что результаты специальной проверки выразятся не только в «чистоте» проверенных помещений, но и в общем повышении уровня защиты информации на предприятии.

5.2. Специальные исследования

Рассматривая вопросы защиты информации, мы убедились в том, что любая защита эффективна только тогда, когда она обеспечивается проведением комплекса мероприятий по защите информации от утечки по всем возможным каналам и постоянным контролем эффективности принятых мер и средств защиты. Возможные технические каналы и принципы их функционирования были рассмотрены в первой главе, в четвертой главе анализировались различные технические средства активной и пассивной защиты. Однако для грамотного использования этих средств необходимо оценить степень защищенности Вашего помещения или технических средств, которое Вы собираетесь защищать. Определить соответствие уровня защиты нормативным требованиям. Эти требования изложены в ряде нормативно-технических документов (НМД, как правило, закрытых), и соответствие реальной защиты установленным требованиям определяется в ходе специальных исследований. Данное пособие носит открытый характер и разрабатывалось на основе открытой общедоступной литературы. Так как без освещения вопросов специальных исследований рассмотрение вопроса будет неполным, автор решил воспользоваться материалами, которые были еще в 2005 году опубликованы в нашем пособии «Защита от утечки информации по техническим каналам» (М: Горячая линия — Телеком, 2005), которое было рекомендовано ФСТЭК как пособие для экспертов в области защиты информации. Учитывая, что особых изменений в методах проведения специсследований за этот период не произошло, а основные изменения связаны с появлением новой аппаратуры для автоматизации процесса измерений, на это и будет сделан основной акцент в данном разделе. Прежде чем перейти к основному материалу, рассмотрим общие положения, термины и определения.

5.2.1. Общие положения, термины и определения

Специальные исследования (СИ). Выявление с использованием контрольно-измерительной аппаратуры возможных технических каналов утечки защищаемой информации от основных и вспомогательных

технических средств и систем и оценка соответствия защиты информации требованиям нормативных документов по защите информации (ГОСТ Р 51863-2007. Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования. ГОСТ Р 51583-2000. Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения).

Следовательно, этот термин может использоваться для любых инструментальных измерений, целью которых является выявление и измерение сигналов в возможных каналах утечки информации так называемых опасных сигналов, некоторые расчетные операции с ними и последующее сравнение рассчитанных величин с нормированными величинами. Довольно широко распространившееся в последнее время толкование этого термина как измерения только в области побочных электромагнитных излучений вычислительной техники является неоправданным ограничением.

Опасный сигнал — это сигнал, который содержит подлежащую защите информацию (ОСТ В1 00464-97. Защита информации об авиационной технике и вооружении от иностранных технических разведок).

Под опасными сигналами понимаются любые сигналы, независимо от их физической природы (электрические в проводниках, механические в жидких, твердых или газовых средах, электромагнитные любой частоты и т. д.), в каналах возможной утечки, несущие скрываемую, защищаемую информацию. Как правило, при проведении СИ реальная информация заменяется имитирующей, тестовой.

Нормы (например, эффективности защиты информации). Значения показателей эффективности защиты информации, установленные нормативными документами (ГОСТ Р 50922-96. Защита информации. Основные термины и определения).

В общедоступном понимании это некое численное значение (иногда может задаваться графически), установленное соответствующим регламентирующим документом, при превышении значения которого опасным сигналом данный канал утечки считается существующим, т. е. разведдоступным. В основном, эти значения дифференцированы в зависимости от важности и формы существования защищаемой информации (цифровая, аналоговая, различным образом кодированная и т. д.), а также вида информации (речевая, телевизионная, средств вычислительной техники и т. д.). Нормированные значения задаются и измеряются практически всегда на границе КЗ.

Побочные электромагнитные излучения и наводки (ПЭМИН) — электромагнитные излучения технических средств обработки защищаемой информации, возникающие как побочное явление и вызванные электрическими сигналами, действующими в их электрических

и магнитных цепях, а также электромагнитные наводки этих сигналов на токопроводящие линии, конструкции и цепи питания (ОСТ В1 00464-97. Защита информации об авиационной технике и вооружении от иностранных технических разведок).

По сути, это опасные сигналы, представляющие собой электромагнитное излучение, сопровождающее процессы «движения» защищаемой информации по цепям и узлам технических средств, а также наводки этого излучения на любые линии. В этот же термин включаются излучения всех генераторов, как штатных, так и «паразитных». Термин распространяется на все области СИ, включая акустоэлектрические преобразования, побочные излучения в речевой области и излучения различных цифровых устройств.

Речевая информация — акустическая информация, источником которой является человеческая речь (ОСТ В1 00464-97. Защита информации об авиационной технике и вооружении от иностранных технических разведок).

Акустоэлектрические преобразования (АЭП) — канал утечки речевой информации, обусловленный преобразованием акустических колебаний в электрические и обратно и распространением этих колебаний в различных присущих им средах (ОСТ В1 00464-97. Защита информации об авиационной технике и вооружении от иностранных технических разведок).

Это группа каналов утечки, образующихся при проявлении физических эффектов и одновременно воздействии акустических речевых сигналов на цепи, узлы, элементы различных устройств, что вызывает появления в них соответствующих электрических сигналов. Часто применяемый синоним — *микрофонный эффект.* Подразделяются на прямые АЭП (в диапазоне частот речевого сигнала, как правило, 300...3400 Гц) и модуляционные АЭП (в радиодиапазоне от 10 кГц до 1200 МГц). Первые характеризуются тем, что появляющиеся опасные сигналы имеют тот же частотный диапазон, что и воздействующие акустические колебания; вторые являются результатом модуляции (включая параметрическую) частот любых генераторов сигналами прямого АЭП. Опасные сигналы, порожденные прямым АЭП, распространяются, как правило, в силу своей низкочастотности и малых величин, по отходящим линиям. Модуляционные АЭП могут распространяться как по линиям, так и по эфиру. В регламентирующих документах используется термин *электроакустические преобразования*, что нарушает физическую логику причины и следствия. В этих процессах первичными причинами являются именно акустические колебания.

Акустика и вибрация (АВАК). Неполный синоним: *канал утечки речевой информации.* Это совокупность источника речевой инфор-

мации, среды распространения акустических сигналов и акустического приемника, обусловливающая возможность перехвата речевой информации (ОСТ В1 00464-97. Защита информации об авиационной технике и вооружении). Совокупность каналов утечки акустической (речевой) информации в форме существования в виде механических колебаний и одновременно весь комплекс СИ в этой области.

Основные технические средства и системы (ОТСС) — технические средства и системы, а также их коммуникации, используемые для обработки, хранения и передачи конфиденциальной информации. В контексте настоящего документа к ним относятся АС различного уровня и назначения на базе СВТ, средства и системы связи и передачи данных, включая коммуникационное оборудование, используемые для обработки конфиденциальной информации (СТР-К).

Общий термин, объединяющий любые технические средства, предназначенные для обработки, хранения или пересылки закрытой информации (любой и в любой ее форме). Например, система звукоусиления в зале, если она используется при проведении закрытых мероприятий, ПЭВМ, обрабатывающая закрытые данные, видеопроектор для показа закрытых изображений и т. д.

Вспомогательные технические средства и системы (ВТСС) — технические средства и системы, не предназначенные для передачи, обработки и хранения конфиденциальной информации, устанавливаемые совместно с основными техническими средствами и системами или в защищаемых помещениях (Специальные требования и рекомендации по защите конфиденциальной информации, утвержденные Гостехкомиссией России №7.2 от 02.03.2001 г, далее СТР-К).

Это любые технические средства, размещенные в защищаемых помещениях и/или рядом с ОТСС, но не предназначенные для обработки, хранения или пересылки закрытой информации (любой и в любой ее форме). В определение ВТСС, однако, не включены воздействующие на них акустические поля, которые образуются голосом человека, техническими средствами и представляют наибольшую опасность возможной утечки информации при исследовании ВТСС.

Одно и то же ТС может быть одновременно, но для различной информации, принадлежать и к ВТСС, и к ОТСС. Например, ПЭВМ может являться ОТСС для обрабатываемой на ней информации и одновременно ВТСС для присутствующей в помещении речевой информации.

Защищаемые помещения (ЗП) — помещения (служебные кабинеты, актовые, конференц-залы и т. д.), специально предназначенные для проведения конфиденциальных мероприятий (совещаний, обсуждений, конференций, переговоров и т. п.) (СТР-К).

Помещение, в котором присутствует защищаемая речевая информация. В соответствии с регламентирующими документами этот термин применяется, когда защищаемая информация имеет конфиденциальный характер. В случае информации, относящейся к государственной тайне, говорят о *выделенном помещении (ВП)*.

Ограждающие конструкции (ОК). Для ЗП (ВП) — все 4 стены (перегородки) и перекрытия пола и потолка, а также окна и двери. Важно понимать и постоянно помнить, что ОК рассматриваются во всех шести направлениях (четыре стены, пол и потолок).

Инженерные конструкции (ИК). Для ЗП (ВП) — все инженерные системы — отопление, вентиляция, кондиционирование, водоснабжение, канализация и т. д., которые находятся в помещении, т. е. любые системы, по элементам которых могут распространяться акустические или вибрационные колебания.

Контролируемая зона (КЗ) — пространство (территория, здание, часть здания), в котором исключено неконтролируемое пребывание сотрудников и посетителей организации, а также транспортных, технических и иных материальных средств.

Границей КЗ могут являтьсяр периметр охраняемой территории организации либо ограждающие конструкции охраняемого здания или охраняемой части здания, если оно размещено на неохраняемой территории.

В отдельных случаях на период обработки техническими средствами конфиденциальной информации границы КЗ временно могут расширяться. При этом должны приниматься организационные и технические меры, исключающие или существенно затрудняющие возможность ведения перехвата информации в этой зоне (СТР-К).

В контексте данного материала этот термин используется в несколько измененном значении. Контролируемая зона — это область пространства вокруг объекта (ЗП, ВП или ОТСС), за пределами границ которой в соответствии с установленными требованиями невозможна утечка защищаемой информации, точнее — необходимо обеспечить невозможность ее утечки. При такой формулировке происходит как бы слияние двух терминов, а именно собственно *КЗ и зоны R2*.

Границы КЗ определяются, описываются и утверждаются заказчиком до проведения СИ. Их определениене входит в задачу проведения специальных исследований. Данная информация должна выдаваться в техническом задании на проведение СИ.

Система активной защиты (САЗ). Любая система зашумления, независимо от ее назначения и построения. Это может быть система электрического линейного зашумления в речевом диапазоне, система объемного зашумления (электромагнитные шумовые поля) в диапазоне до сотен МГц или система вибрационного зашумления.

Антенно-фидерные устройства (АФУ). Под такими устройствами, в рамках данного материала, подразумеваются все элементы антенного тракта измерительной системы, с помощью которой проводятся СИ (собственно антенны, токовые трансформаторы, кабели, предусилители, пробники и т. д.), т. е. все, что является источником сигнала для измерительного прибора.

5.2.2. Постановка задачи на проведение специальных исследований

Как следует из определения термина, задачей специальных исследований (СИ) является выявление и измерения сигналов в потенциальных каналах возможной утечки информации — опасных сигналов (ОС). Причем, как правило, первая часть задачи является определяющей по затратам времени и сил. Учитывая, что величины ОС весьма малы (как по сравнению с другими, «рядом» существующими сигналами, так и по сравнению с уровнем помех), задача их надежной идентификации совсем не тривиальна. Ошибка на этом этапе неизменно приводит либо к пропуску ОС, либо к завышению результатов.

Весьма желательным, а скорее обязательным, условием является и функционирование исследуемого узла, блока, устройства в режиме, одновременно максимально близком к обычному рабочему и в то же время в режиме, имеющем ряд специфических особенностей, в тестовом режиме.

Вернёмся к приведённой ранее модели технического канала утечки информации.

Если рассмотреть задачу защиты информации от возможной утечки в понятиях, свойственных приведенной модели, то в точке размещения потенциального противника необходимо обеспечить такое отношение сигнал/шум, которое не позволит противнику восстановить защищаемую информацию (существенно затруднит получение информации). При этом отношения сигнал/шум, при которых вероятность восстановления единицы информации принимает заданные значение, характеризует так называемый *параметр защищённости* объекта.

Для дальнейшего рассмотрения необходимо понимание того, что отношение сигнал/шум всегда рассматривается в точке возможного перехвата, т. е. в точке «конца» канала утечки. Эта точка, в соответствии с принятыми терминами и положениями, в подавляющем числе рассматриваемых случаев находится на границе контролируемой зоны (КЗ) объекта.

Рассматривая математическое выражение, описывающее отношение сигнал/шум, нетрудно сделать вывод, что практическая задача достижения требуемого его значения может быть решена трояко.

Прежде всего, напомним, что уровень естественных шумов (помех) в канале принят постоянным в любой его точке. При этом условии для решения задачи необходимо либо уменьшать сигнал передатчика, либо увеличивать затухание сигнала в канале. Третий вариант — увеличивать уровень шума в канале (в этом случае рассматриваются искусственно созданные шумы).

На практике в общем случае для обеспечения защищённости применяют все перечисленные способы либо их комбинации.

5.2.3. Содержание специальных исследований

Задача СИ как комплекса работ, позволяющего установить, возможна ли утечка информации в данном канале, сводится к измерению сигналов передатчика и пересчету измеренных значений к величине, которая может поступить на вход оптимально адаптированного к данному виду информации приемника потенциального противника.

Этот расчёт выполняется исходя из принятого (заданного нормативными документами) закона затухания сигналов в канале либо затухание в канале нужно измерить и наложить на сигнал, чтобы рассчитать его значение на дальнем (от передатчика) конце канала. Затем необходимо вычислить отношение сигнал/шум в точке возможного перехвата. После этого сравнить полученные значения с величинами, записанными в нормативных документах. При этом уровень шумов в канале может быть задан нормативными документами или его придеться измерять.

В соответствии с требованиями нормативных документов специальные исследования подразделяются на две основных группы: стендовые (лабораторные) СИ и объектовые СИ.

При проведении исследований разные группы каналов утечки могут исследоваться тем или другим методом. При этом методы могут быть предписаны или решение на их выполнение принимается исследователем.

Стендовые СИ проводятся, в основном, для определения специальных свойств ТС в стандартизованных условиях. При этом полученные результаты, как правило, являются справочными, позволяющими первоначально оценить исходную защищённость устройства для дальнейшего оптимального проектирования системы защиты и применения на объекте пассивных и активных средств и мер для защиты информации на объекте.

Объектовые СИ проводятся для оценки защищённости объекта в условиях реальной эксплуатации. При этом до проведения специальных исследований должна быть проведена определенная исходная работа по определению защищаемых помещений, составлены перечни технических средств, размещённых в них (ОТСС, ТСПИ и ВТСС).

Затем выполняется инженерный анализ технических средств и отходящих от них линий. Оценка выделенных помещений (включая граничащих с ними), инженерных и технических коммуникаций и т. д. Задача анализа — выявление потенциально возможных каналов утечки информации исходя из характеристик объектов и требований нормативных документов.

Без проведения такого анализа выполнение СИ бессмысленно, да и просто невозможно. Для обоснования исследования именно выбранных технических каналов утечки и, соответственно, технических средств (ВТСС, ОТСС), конструкций и т. д., краткие результаты анализа должны приводяться в протоколах СИ. Этот анализ, как правило, проводится службами заказчика, совместно со специалистами исполнителя.

Проведение любых СИ основано на замене в техническом канале утечки реального информационного сигнала на некий тестовый сигнал. Такая замена обусловлена тем, что необходимо предотвратить утечки реальной информации в ходе проведения исследований, а также тем, что тестовый сигнал в большинстве случаев может иметь значительно более высокий уровень, чем реальный ОС. Исходя из этого, чем выше уровень сигнала, тем меньше влияние помех при его измерениях, следовательно, ниже необходимая чувствительность измерительной аппаратуры и меньше её стоимость.

Тест-режим (тест-сигнал) применяется для создания имитационного опасного сигнала такого уровня, чтобы его можно было уверенно выделить на фоне любых помех в канале либо придать определенную «окраску» тестовому сигналу для его надежного опознавания оператором или автоматикой исследовательских измерительных комплексов. Зачастую приходится решить обе эти задачи. Исходя из этого понятно, какую важную роль играют правильно выбранные тест-сигналы, а также разработка и проведение тест-режимов (тест-программ). Применяемые тест-режимы должны быть описаны в протоколе СИ, если они не оговорены методиками, при этом описание должно включать основные параметры тест-сигналов. При необходимости приводятся осциллограммы тест-сигналов в цепях исследуемого технического средства.

В ряде случаев необходим предварительный анализ исследуемого объекта (технического средства), с целью выявления «слабых мест». Специалист-исследователь должен четко представлять себе, какие именно элементы, узлы, блоки имеют наибольшую вероятность образования каналов утечки, и обязан сосредоточить свое внимание именно на них. Без этой предварительной «оптимизации» процедура СИ становится недопустимо долгой и дорогостоящей. Этот анализ

должен быть изложен и обоснован в соответствующих разделах протоколов, при этом достаточно подробно указывается, какие элементы объекта подвергаются исследованию и почему именно они.

Вся эта предварительная работа может быть сокращена в заметной степени с учётом накопленного опыта, статистики, ясного понимания физических процессов в аппаратуре, средах распространения сигналов и функционирования средств измерений.

После обнаружения тестовых сигналов они должны быть измерены и определены их величины. При этом необходимо обратить внимание на то, что для измерения необходимо иметь и использовать определенные для этого средства измерения. В соответствии с Федеральным законом «Об обеспечении единства измерений» для этих целей могут применяться только средства, введенные в Госреестр средств измерений и имеющие свидетельство о поверке с непросроченным сроком действия. Необходимо отметить, что в случаях применения не стандартных измерительных приборов общего назначения, а специализированных измерительных систем и комплексов они должны иметь сертификат ФСТЭК России. Перечень средств измерений, использованных при проведении СИ, должен приводиться в протоколе вместе со ссылками на свидетельства о поверке (калибровке).

Заказчик работы (специальных исследований) может потребовать от Исполнителя предоставления копий сертификатов о включении средства измерений в Госреестр и свидетельств о поверке, что является его правом. При этом, формально, СИ, которые выполнены с использованием приборов, не включенных в Госреестр, силы не имеют и не могут являться основанием для аттестации объекта. Информация о средствах измерения, включенных в Госреестр, может быть получена по справочным телефонам Всероссийского научно-исследовательского института метрологической службы (ВНИИМС).

Измеренные значения приводятся в протоколе, как правило, в форме подробных таблиц. При этом в качестве приложений должны быть представлены описания условий измерений, схемы измерений и/или в ряде случаев фотографии, демонстрирующие взаимное размещение исследуемого объекта и элементов измерительной системы. Приводимая информация должна быть достаточно полной для того, чтобы можно было полностью восстановить все условия для проведения контрольных измерений.

После измерения величин опасных сигналов в ряде случаев необходимо произвести расчеты в соответствии с действующими методиками для перевода измеренных значений в ту форму и к тем величинам, которые подлежат сравнению с нормированными значениями. В протоколе приводится весь процесс расчета, включая промежуточные

значения, с подробным описанием всех сделанных допущений, упрощений и т. д.

Зачастую, сигнал не может быть выявлен на фоне шумов, здесь имеется в виду, как правило, сумма внешних шумов и шумов измерительного тракта. В данном случае расчет производится «по шумам», т. е. опасный сигнал принимается равным шумам канала и оценка производится по этим значениям. Это относится к любым видам специальных исследований независимо от физической природы опасных сигналов, видов разведки и оцениваемых каналов утечки. Понятно, что при таком подходе результат «оценки по шумам» будет зависеть от параметров средств измерения. Использование низкочувствительной, «шумящей» аппаратуры может привести к существенному завышению результатов специальных исследований, превышению значений измеренных (расчетных) параметров на границе контролируемой зоны установленным нормам, хотя на самом деле опасности утечки и не существует. Именно поэтому очень много зависит от выбора средств измерения.

Заключительным этапом специальных исследований является сравнение полученных рассчитанных значений опасных сигналов с соответствующими нормами и формулировка выводов. В большинстве своем эти формулировки носят краткий, единый по форме и содержанию, однозначный характер. В отдельных случаях необходимо указывать допуски на параметры технических средств или внешних сетей.

Пример 1.

Значения опасных сигналов в телефонной линии **не удовлетворяют** действующим нормам для ... категории объекта.

Значения опасных сигналов **удовлетворяют** действующим нормам при штатном функционировании электросети и **не удовлетворяет** действующим нормам при ее аварийных или преднамеренных (в том числе подмене) отключениях для ... категории объекта.

Пример 2.

Значения опасных сигналов в линии электропитания как при штатно функционирующей электросети, так и в случаях ее отключения, **удовлетворяет** действующим нормам для ... категории объекта.

Возможно включение в окончательные, сводные выводы протокола (заключения) рекомендаций, которые направлены на исключение (блокирование) обнаруженных каналов утечки.

5.2.4. Специальные исследования в области защиты речевой информации

Специальные исследования в этой области в зависимости от формы существования опасных сигналов подразделяются: на исследования в области акустики и вибраций, исследования в области акустоэлектрических преобразований и исследования ВЧ навязывания (ВЧ

облучения). Так как эти исследования существенно отличаются и составом средств измерения, и многим другим, то целесообразно рассматривать их последовательно и раздельно.

Так как данное пособие носит открытый характер и в нём рассматриваются вопросы защиты информации конфиденциального харатара, а исследования ОТСС имеют ряд особенностей, то в данном пособии они не рассматриваются.

В данном пособии рассматриваются только вопросы специальных исследований акустоэлектрических преобразований ВТСС.

Исследования в области акустики и вибраций (зачастую в нормативной и другой документации используется термин «виброакустика», который объединяет смысловое содержание терминов «акустика» и «вибрация») проводятся, как правило, по отношению к защищаемым (выделенным) помещениям. Следовательно, такие специальные исследования могут быть только объектовыми. Поэтому объектом исследований в этой области будут являться ограждающие конструкции помещения, все отходящие короба, трубопроводы и другие инженерные конструкции.

Методика проведения исследований и нормы (параметры) защищенности в этой области определяются в настоящее время для информации конфиденциального характера соответствующим приложением к СТР-К.

Рассмотрим поэтапно весь комплекс работ, составляющих специальные исследования в области акустики и вибраций (СИ АВАК) для выделенного помещения. Рассмотрение комплекса мероприятий будем рассматривать в последовательности, в которой рекомендуется составление протокола СИ АВАК.

Название организации, выполняющей СИ (лицензиата ФСТЭК), ссылка на его лицензии и название объекта СИ.

Объекты контроля (ЗП) и их краткое описание.

Уровень защиты для каждого из них.

Размещение ЗП.

Список помещений, граничащих с ЗП (во всех направлениях, «в сфере»). В этом разделе рекомендуется приводить планы ЗП, их размещение по отношению к смежным помещениям.

Перечень ограждающих конструкций (ОК).

Описание элементов ЗП необходимо выполнять в полном объеме и со всей серьёзностью. При этом сформулированное функциональное и полное описание позволяет заметно уменьшить возможность ошибок за счёт неоптимального выбора размещения точек контроля и их количества.

Ограждающие конструкции. Анализ ограждающих конструкций должен начинаться, прежде всего, с оценки их подробного структур-

ного построения. Все стены, перегородки, перекрытия должны быть подробно описаны. Это необходимо для того, чтобы обосновать проведение (или отказ от проведения) конкретных акустических или вибрационных измерений. Понятно, что измерять акустическую защищенность капитальной стены (кирпичная кладка 650 мм, штукатурка 15 мм, обрешётка (каркас) — деревянный брус 50×50 мм, минвата 50 мм, декоративная ДСП 20 мм) бессмысленно. А защищенность лёгкой перегородки (гипсокартон 12,5 мм, металлический профиль 75×40 мм, зазор 100 мм, гипсокартон 12,5 мм, обои) оценивать придется обязательно.

При описании ограждающих конструкций особое внимание необходимо уделить имеющимся проемам, проломам, трещинам, зазорам. Каждый из таких паразитных «звуководов» требует контрольного замера, так как способен свести почти к нулю защищенность любой ограждающей конструкции.

Особенно важно выявить, установить размещение возможных швов, стыков монолитных конструкций, так как именно они чаще всего и являются «слабым звеном». Кроме того, они же могут в значительной степени определять эффективность систем активной защиты (вибрационного зашумления), так как сильно задерживают распространение виброколебаний. Отсутствие или наличие таких неоднородностей в ограждающих конструкциях должно оговариваться в протоколе отдельно. Примеры описания ограждающих конструкций и их измерений приведены в Приложении к настоящему пособию.

Окна. Описание окон должно быть не менее подробным. Поскольку от вида остекления (стекло, стеклопакет), материала рам и оконной коробки, числа стекол, размеров и количества отдельных створок, способов крепления стекла или стеклопакета в раме зависит количество контрольных точек измерений, а следовательно, и объем СИ, затраты на них. Особенно внимательно, впрочем, как и во всех СИ АВАК, должны быть выявлены и описаны возможные щели, неплотности прилегания рамы к коробке и т. д. Всё это паразитные звуководы. Особенно важной эта информация становится при проектировании систем САЗ. Более подробно типовые варианты размещения контрольных точек на остеклении окон будут рассмотрены далее.

Дверные проёмы. При описании дверных проёмов наиболее важным является описание материалов, структуры и конструкции дверных полотен, выявление неплотностей их прилегания к дверной коробке. Обязательным является указание наличия зазоров между нижним торцом дверного полотна и полом (особенно при отсутствии порога). При наличии двойной двери с тамбуром весьма важно описание размеров тамбура и тех материалов, из которых он выполнен. Анализируя описание дверного проёма, выполненное грамотно, специалист

способен с точностью до 6...8 дБ предположить вносимое им в акустический сигнал затухание. Это служит дополнительной проверкой корректности выполненных измерений. Большое отклонение величин при измерении от ожидаемых должно насторожить исследователя и подтолкнуть его на поиск причин отклонения. При этом причины расхождения всегда должны быть найдены и объяснены.

Инженерные конструкции. Подробное описание воздуховодов, вентиляционных каналов, систем отопления, водоснабжения, канализации, каналов и коробов подводки различного рода проводов и кабелей. Основное внимание в этой части следует уделить информации, помогающей определить границы зоны для канала непреднамеренного прослушивания (например, ближайшие к ЗП окна системы вентиляции). Это также важно в современных условиях и для определения границ КЗ (особенно по трубопроводам водоснабжения, отопления, канализации и т. д.).

Контролируемая зона. Описание конкретного помещения с привязкой к потенциальным каналам утечки. При исследовании помещения прежде всего должны быть определения конкретные границы контролируемой зоны, причем раздельно для акустических (включая непреднамеренное прослушивание) и вибрационных каналов. При определении терминологии было отмечено, что информация о границах контролируемой зоны должна быть подготовлена до начала специальных исследований заказчиком и ее подготовка не входит в комплекс специальных исследований. Это исходные данные заказчика исследований.

Так, например, граница КЗ для акустической речевой информации (за счет непреднамеренного прослушивания) может пройти по ограждающим конструкциям, а в системе вентиляции — по плоскости вентиляционной решетки в ближайшем к ЗП помещении напротив. А может пройти и по технологическому окну в вентиляционном коробе в фальшпотолке коридора непосредственно рядом с выделенным помещением. Внешняя стена выделенного помещения (стена здания), включая окна, может быть границей контролируемой зоны, если это первый этаж, а если это более высокий этаж и потенциальный противник не может находиться вблизи нее, то в этом направлении канал утечки (акустический, за счет непреднамеренного прослушивания) может отсутствовать. Вариантов может быть много, и каждый является основанием для проведения или непроведения измерений в том или ином направлении.

Аналогично анализируются потенциальные вибрационные каналы утечки. Так, например, при наличии собственного расположенного в пределах контролируемой зоны теплопункта (котельной) с замкнутой

схемой циркуляции теплоносителя система отопления вообще не образует канала утечки. А при наличии прямого городского теплоснабжения придется решать, где пройдет граница контролируемой зоны для данного канала — по трубам на выходе из здания или по трубам при выходе из выделенного помещения. Разница для специальных исследований весьма существенная, тем более для организации системы защиты.

Вид проводимого контроля (аттестационный или текущий).

Возможные потенциальные злоумышленники, которым осуществляется противодействие, их возможности и виды каналов утечки, а также их конкретные направления, подлежащие инструментальному контролю.

Проведенный анализ позволит определить все основные элементы защищаемых помещений, которые должны быть инструментально исследованы (измерены).

После определения всех основных элементов защищаемых помещений, которые должны быть инструментально исследованы, необходимо определить порядок проведения исследований, размещение средств контроля (различных датчиков) на различных поверхностях, измерительную аппаратуру и рекомендуемые меры и средства защиты, в первую очередь активные, т. е. системы акустического и/или вибрационного зашумления, а затем пассивные типа звукопоглощающих покрытий, прокладок, обшивок, уплотнителей и т. д. Кроме того, в данном разделе рекомендуется приводить фотографии и/или схемы размещения колонок или вибровозбудителей зашумления, указывать схемы их подключения к генераторам и другую информацию, облегчающую выбор конкретных точек измерения с целью оценки эффективности систем защиты.

Перечень измерительной аппаратуры. Основные характеристики и параметры измерительной аппаратуры, а также активных и пассивных средств защиты были достаточно подробно изложены в 4-й главе.

Таблицы результатов измерений и расчета показателя противодействия. В данном разделе приводятся краткие условия проведения измерений, размещения конкретных точек измерений и элементов измерительного комплекса. Рекомендуется приводить фотографии размещения элементов измерительного комплекса по отношению к измеряемым конструкциям или давать схемы их размещения. Как правило, это проще и информативнее, чем словесное описание. Для конкретных точек, отличающихся по методике замера от других, рекомендуется описывать эти отличия.

В соответствии с методикой, приведённой в нормативно-методических документах, рассчитываются отношения сигнал/шум в каждой

октавной полосе, а если хоть одно из них не соответствует норме, то рассчитывается значение словесной разборчивости.

В Приложении к настоящему пособию приведены примеры таблицы измерений и расчетов отношений сигнал/шум и значений словесной разборчивости речи (*параметров защищённости*).

Заключение. В этом разделе приводятся сводные выводы по защищенности (или незащищенности) всех ограждающих конструкций и инженерных коммуникаций исследованных ЗП и эффективности эксплуатируемых средств активной защиты.

Рассмотрев в общем вопросы исследования в области акустики и вибраций, необходимо рассмотреть положения методики и средства измерения, которые используются для этих целей. Вся действующая методика измерений в области акустики и вибраций основана на измерении двух величин — звукового давления (в воздушной среде) и виброускорения (на поверхности твердого тела). Оба параметра измеряются специализированными приборами — шумомерами с подключаемыми к ним первичными преобразователями — микрофоном и акселерометром. Дополнительно необходим источник акустического тест-сигнала, т. е. генератор-усилитель с акустическим излучателем — колонкой. Поскольку чаще всего измерения проводятся на шумовом тест-сигнале (что не исключает и других сигналов), то источник желательно иметь «шумовой». Звуковое давление, развиваемое на расстоянии 1 м тестовым источником, желательно иметь не менее 100 дБ. При меньшем акустическом давлении выделение опасных сигналов с другой стороны оцениваемой конструкции с заметным затуханием на фоне обычных помех достаточно сложно или вообще невозможно. Крайне желательно иметь возможность гибко регулировать амплитудно-частотные характеристики источника. Зачастую бывает необходима возможность увеличения уровня сигнала в заданной полосе частот.

Шумомер должен быть по классу точности не ниже II класса (как и входящие в его состав измерительный микрофон и акселерометр).

В настоящее время ещё используется достаточно большое количество шумомеров фирмы RFT (которые в свое время производились в ГДР) моделей 00 017, 00 23, 00 019 и др. Это достаточно удобные, малогабаритные носимые приборы I—II классов. Применяются и отечественные аналоги (шумомеры серии ВШВ). Вполне успешно эксплуатируются и различные шумомеры разных моделей, известной фирмы B&K. По сути, независимо от того кто производитель прибора, важно одно, чтобы он отвечал необходимым требованиям, был исправен, поверен и числился в Госреестре.

К микрофонам особых требований не предъявляется, лишь бы они были достаточной точности. Практически все сейчас используют

стандартные полудюймовые конденсаторные микрофоны. Моделей таких микрофонов огромное количество и перечислять их нет особой необходимости. Нужно отметить только, что использование в таких микрофонах поляризующего напряжения (обычно 200 В) и высокое выходное сопротивление самого микрофонного капсуля приводят к тому, что эксплуатировать их приходится при непосредственном подключении к предусилителю без соединительных кабелей. При этом сам выносной предусилитель связан с шумомером достаточно толстым, многожильным кабелем, который далеко не всегда можно просунуть в какую-нибудь узкую щель. Весьма эффективным выходом из этого положения является применение микрофонов ICP-стандарта, которые малогабаритны, включают в свой состав предусилитель и имеют весьма низкие (от единиц до сотен Ом) выходные сопротивления. Их питание производится по сигнальному коаксиальному кабелю. Этот кабель может быть весьма тонким и гибким. Длина кабеля может доходить до десятков метров.

Примерно тоже можно сказать и об акселерометрах. Для измерений можно использовать любую модель, если она исправна и поверена, при этом неоходимо учитывать и дополнительные требования. Масса акселерометра должна быть минимальной, чтобы не вносить заметную погрешность при установке на стекло (желательно не более первого десятка грамм), а его чувствительность — не ниже 50 мВ/м·с^2. Для измерений в особо «тихих» условиях уровень собственных шумов акселерометра должен быть минимально возможным.

Для зарядовых акселерометров паспортную чувствительность нетрудно пересчитать через входные параметры предварительного усилителя. Собственная механическая резонансная частота акселерометра должна лежать выше рабочего диапазона частот (желательно выше 11 кГц). Это особенно важно при установке акселерометра на «игле», когда его резонансная частота резко снижается.

Кроме этого, обязательным элементом комплекса средств измерения является акустический калибратор (эталон звукового давления). Моделей таких калибраторов вполне достаточно. Это и приборы раннего выпуска PS-101, 0005 (RFT), современные CAL-200, CAL-250 (L&D), несколько моделей B&K, отличающиеся, практически, только ценой. Может применяться любая из этих моделей, соответствующим образом поверенная. Калибровка микрофонов необходима перед каждой серией измерений. Особенно это важно при изменении температуры окружающей среды, атмосферного давления (например, при измерениях в двух помещениях, разделенных несколькими этажами). При этом наиболее целесообразно откалибровать приборы до и после проведения измерения.

Рис. 5.17. Программно-аппаратный комплекс «Спрут-11»

В настоящее время для измерения и анализа степени защищенности объекта нашли широкое применение автоматизированные измерительные системы (комплексы). Таких систем в настоящее время существует несколько. Это комплексы «Аврора», ВЕ-100, «Гвоздика», «Спрут», «Шёпот».

Практически все перечисленные комплексы реализуют утвержденную методику измерений и имеют соответствующие сертификаты ФСТЭК РФ. Также у комплексов имеются метрологические сертификаты, как правило, военного средства измерения. В отношении комплекса «Гвоздика» сведения о сертификатах ФСТЭК и метрологическом отсутствуют.

Дадим краткую характеристику используемых средств измерения.

Программно-аппаратный комплекс «Спрут-11» (рис. 5.17) предназначен для проверки выполнения норм эффективности защиты речевой информации от её утечки по акустическому и виброакустическому каналам, а также за счет низкочастотных наводок на токопроводящие элементы ограждающих конструкций зданий и сооружений и наводок от технических средств в речевом диапазоне частот, образованных за счет акусто-электрических преобразований. Управление комплексом осуществляется по радиоканалу. Связь между модулями комплекса осуществляется по радиоканалу (Wi-Fi) в цифровом виде. Дальность связи зависит от условий работы. Минимальная дальность в зависимости от типа материалов здания (сооружения) может составлять от 5 до 100 м. В состав комплекса входят:

- измерительный микрофон, который является датчиком для измерения уровней акустических сигналов (подключается к измерительному модулю при помощи специального кабеля), и микрофонный предусилитель. В зависимости от комплекта поставки в составе комплекса могут использоваться различные измерительные микрофоны;

- акселерометр АР-98, который предназначен для измерения уровней виброускорения. Он имеет встроенный усилитель заряда, поэтому требует ICP-питания (обеспечивается измерительным модулем). В комплект акселерометра входит соединительный коаксиальный кабель и адаптер для подключения к измерительному модулю;
- измерительные усилители, которые предназначены для подключения к измерительному модулю различных источников низковольтных сигналов, в том числе измерительных антенн, пробников, циллографических щупов, токосъемников и т. п. В состав комплекса входит два измерительных усилителя: усилитель № 1 SZA1 ($K_{\text{ус}}$ = 40 дБ) представляет собой инструментальный усилитель с низким уровнем собственных шумов; усилитель № 2 SZA2 ($K_{\text{ус}}$ = 40 дБ) оборудован встроенным режекторным фильтром на 50 Гц с ослаблением основной гармоники 56 дБ, что позволяет уменьшить уровень нежелательного сигнала, наведенного в исследуемой линии от сети 220 (380) В 50 Гц, в 200 раз;
- модуль источника тестового акустического сигнала, который используется для создания тестового акустического сигнала при проведении измерений звукоизоляционных и виброизоляционных параметров помещения, эффективности систем виброакустического зашумления и других исследований. Данный модуль (ультракомпактный ноутбук) генерирует следующие виды сигналов: непрерывный гармонический сигнал на частотах в диапазоне от 1 до 20000 Гц; белый шум; розовый шум. При использовании белого или розового шума, АЧХ сигнала может быть откорректирована с помощью встроенного эквалайзера.

Управление источником тестового акустического сигнала осуществляется вручную или дистанционно по радиоканалу с использованием подсистемы управления. Для включения генератора необходимо запустить установленную на ПЭВМ (ультракомпактный ноутбук) программу S8ATG. Внешний вид передней панели программы S8ATG приведен на рис. 5.18.

Специальное программное обеспечение «Спрут-11» (СПО) предназначено для управления измерительным модулем и модулем источника тестового акустического сигнала, получения результатов измерений, их обработки, отображения и сохранения в необходимом формате, проведения расчетов в соответствии с утвержденной Методикой.

СПО «Спрут-11» состоит из двух частей — измерительной и расчетной. Измерительная часть запускается с рабочего стола ПЭВМ из раздела «Пуск» — «Программы» — Sprut 11. Главное окно измерительной части СПО «Спрут-11» приведено на рис. 5.19.

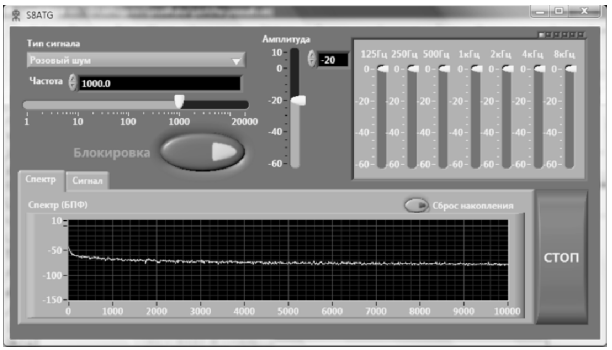


Рис. 5.18. Внешний вид передней панели программы S8ATG

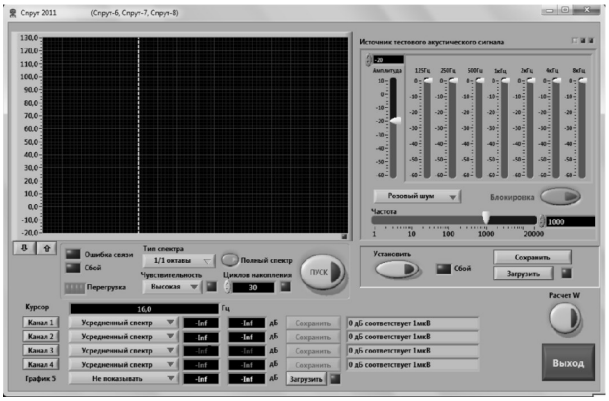


Рис. 5.19. Главное окно измерительной части СПО «Спрут-11»

Главное окно измерительной части программы имеет две основные области: панель измерительного модуля и панель источника тестового акустического сигнала.

Расчетная часть СПО «Спрут-11» (рис. 5.20) запускается с рабочего стола ПЭВМ из раздела «Пуск» — «Программы» — Sprut-2011 — «Расчет W». Данная расчетная часть СПО «Спрут-11» имеет сертификат соответствия действующим нормативно-техническим документам Государственной технической комиссии России НМД АРР № 936.

Комплекс «Шёпот». В состав комплекса входит современный интегрирующий шумомер Larsen&Davis модели 824. Прецизионный интегрирующий шумомер I класса, введенный в Госреестр средств измерений, позволяет выполнять не одно, а большое количество измерений (каждые 125 мс), усредняя результат за установленное оператором время. Такой метод измерения в полной мере соответствует метрологическим стандартам и стандартам по измерениям в облас-

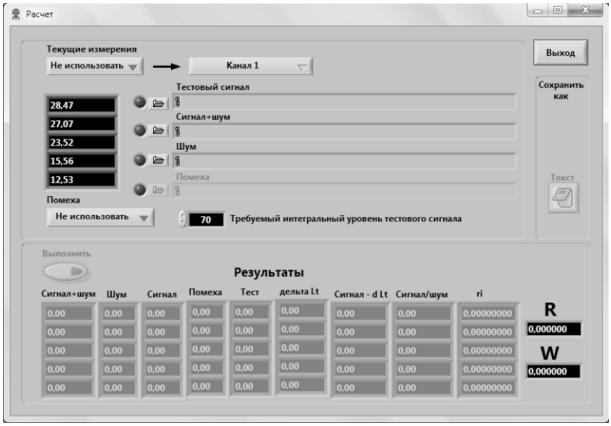


Рис. 5.20. Главное окно расчетной части СПО «Спрут-11»

Рис. 5.21. Общий вид системы «Шёпот»

ти акустики и вибраций. Измерения в последней версии комплекса могут выполняться как в пяти, так и в семи октавных полосах, что соответствует последним требованиям руководящих документов.

Кроме того, система «Шёпот» автоматически выбирает минимальные значения при измерении уровней фоновых шумов (что предписано действующей методикой НМД АРР). Источник тестового акустического сигнала «Шорох-2МИ» имеет семиполосный эквалайзер, позволяющий гибко менять его АЧХ. Прецизионные поверяемые радиоканалы позволяют относить ICP-микрофон и акселерометр на значительное расстояние от комплекса, размещать их практически в лю-

бых труднодоступных местах, в том числе и за стенами помещения и на других этажах. При подключении датчиков на кабелях длина последних составляет до 20 м в штатной комплектации (может быть увеличена или уменьшена по отдельному заказу).

Опционно в комплекте системы «Шёпот» может поставляться высокочувствительный акселерометр PCB352B, незаменимый при измерении вибраций на «тяжёлых» конструкциях (например на фундаментах).

Система «Шёпот» позволяет выполнять в едином цикле измерения уровня тестового сигнала до исследуемой конструкции и после неё. Ведет базу данных по всем выполненным измерениям, напоминает оператору о необходимости описать все элементы выделенных помещений для протокола, значительно облегчает настройку и оптимизацию средств активной защиты в выделенных помещениях.

Модифицированный вариант системы «Шёпот-Т» имеет меньшие габариты, стоимость, ряд других отличий и преимуществ, связанных с заменой шумомера L&D на шумомер «Тритон», который также является шумомером-анализатором спектра I класса, но значительно меньше по массогабаритным показателям и обладает рядом преимуществ.

Вообще применение автоматизированных систем при проведении специальных исследований в области акустики и вибраций предпочтительно, так как их использование исключает многие возможные ошибки оператора, значительно повышает точность измерений и упрощает создание финального протокола.

Программно-аппаратный комплекс «Аргонавт» (рис. 5.22) позволяет автоматизировать измерений при проведении специальных исследований и аттестации объектов информатизации. С помощью комплекса можно решать следующие задачи:

- проведение инженерных исследований и исследований на сверхнормативные побочные электромагнитные излучения;
- оценку защищенности объектов информатизации от утечки речевой информации за счет акустоэлектрических преобразований;
- оценку защищенности объектов информатизации от утечки речевой информации по акустическому и виброакустическому каналам.

Комплекс разработан с учетом требований «Сборника методических документов по контролю защищенности информации, обрабатываемой средствами вычислительной техники, от утечки за счет побочных электромагнитных излучений и наводок (ПЭМИН)» (новая редакция), утвержденного приказом ФСТЭК России от 30 декабря 2005 года; «Сборника нормативно-методических документов по противодействию акустической речевой разведке»; «Сборника методик изме-

Рис. 5.22. Программно-аппаратный комплекс «Аргонавт»

рений и расчета параметров вспомогательных технических средств и систем с целью определения их соответствия установленным нормам на параметры в речевом диапазоне частот», МПСС, 1978 г. Диапазон частот комплекса: 1 Гц...3 ГГц.

В состав комплекса входят:

- анализатор сигналов серии SA86000 для проведения измерений в диапазоне частот от 1 до 50000 Гц и управления высокочастотным анализатором спектра (измерительным приемником);
- анализатор спектра Rohde&Schwarz FSL3.03, рабочий диапазон частот 9 кГц...3 ГГц, с дополнительными опциями: ВЧ предусилитель (R&S FSL-B22), полосовые фильтры с разрешением от 10 до 100 Гц (R&S FSL-B7), источник питания DC 12–28 В (R&S FSL-B30), аккумуляторная батарея NiMH (R&S FSL-B31), измерительный демодулятор АМ/ЧМ/ФМ (R&S FSL-K7);
- головные телефоны для подключения к анализатору спектра;
- комплект активных аттестованных широкополосных измерительных антенн: дипольная АИ5-0 с рабочим диапазоном частот 0,009 ...2000 МГц и рамочная АИР3-2 с рабочим диапазоном частот 0,009...30 МГц;
- аккумулятор с зарядным устройством для подключения комплекта антенн (АИ5-0 и АИР 3-2);
- пробник напряжения «Шмель» с рабочим диапазоном частот от 9 кГц до 300 МГц;
- управляющий Notebook (опционально);
- штатив диэлектрический ШД-1 для крепления и установки антенн с метрологическим сертификатом;
- интерфейсный LAN-кабель с RJ-разъемами для подключения анализатора спектра FSL3.03 к анализатору сигналов серии SA86000;
- стол поворотный диэлектрический с дистанционным приводом;

- эквивалент сети ЭС300, рабочий диапазон частот от 9 кГц до 300 МГц;
- измерительный микрофон;
- измерительный акселерометр;
- источник тестового акустического сигнала;
- источник электропитания проверяемых технических средств;
- активная акустическая система с экранирующим контейнером.

Программно-аппаратный комплекс «Аист» (рис. 5.23) предназначен для выявления акустоэлектрических преобразований в речевом диапазоне частот, выявления свойств микрофонного эффекта, наблюдения, измерения и сохранения амплитудных, временных и частотных характеристик сигналов речевого диапазона частот различной физической природы, а также генерации сигналов речевого диапазона частот задаваемой пользователем формы.

Рис. 5.23. Программно-аппаратный комплекс «Аист»

Анализ сигналов различной физической природы обеспечивается использованием в составе комплекса датчиков различного типа, поддержка которых реализована во встроенном ПО анализатора сигналов SA86001 — основного компонента комплекса.

Анализатор сигналов SA86001 представляет собой стационарный электроизмерительный прибор, построенный на основе технологии виртуальных приборов, в его составе:

- встроенный промышленный компьютер;
- устройства ввода/вывода сигналов со встроенными модулями аналогово-цифрового и цифро-аналогового преобразования;
- устройство управления;
- дисплей;
- блок питания.

Программное обеспечение анализатора сигналов работает под управлением операционной системы Windows.

СПО представляет собой компьютерную программу, реализующую следующие основные функции:

- управление основными модулями анализатора сигналов;
- сбор данных измерений;
- реализация измерительных алгоритмов;
- реализация алгоритмов цифровой обработки данных измерений.
- отображение результатов измерений;
- сохранение результатов измерений.

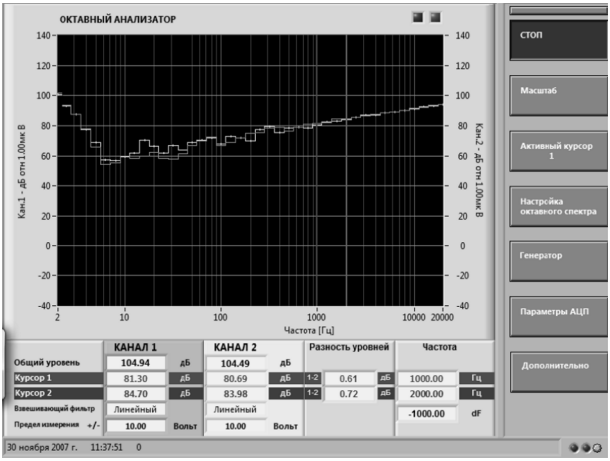


Рис. 5.24. Вид типового окна СПО

Измерительные алгоритмы СПО в базовой конфигурации включают в себя:

- октавный анализ;
- узкополосный анализ на основе алгоритма быстрого преобразования Фурье;
- реализацию функции измерителя шума и вибраций;
- цифровой осциллограф;
- реализацию функции измерителя электромагнитных полей и наводок;
- реализацию функции генератора сигналов различной формы.

Типовое окно СПО изображено на рис. 5.24.

Рассмотрим порядок подключения комплекса при проведении основных операций исследования, а именно: выявление микрофонного эффекта; исследование телефонной линии; исследование цепи питания.

Выявление микрофонного эффекта. Схема подключения комплекса показана на рис. 5.25. Вход акустической колонки подключается к выходу генератора программно-аппаратного комплекса (ПАК) «Аист», вход микрофона подключается к входу ПАК «Аист», исследуемый объект устанавливается между акустической колонкой и микрофоном.

Исследование телефонной линии. При исследовании телефонной линии комплекс подключается следующим образом (рис. 5.26): адаптер для подключения телефонных линий подключается к автономному источнику питания, а к входу адаптера подключается кабель исследуемой телефонной линии, при этом на вход ПАК «Аист» подключается выход адаптера.

Рис. 5.25. Схема подключения комплекса при выявлении микрофонного эффекта

Рис. 5.26. Схема подключения комплекса при исследовании телефонной линии

Исследование цепи питания. При исследовании цепи питания комплекс подключается достаточно просто (рис. 5.27): вход адаптера подключается к сети 220 В, а выход адаптера подключается к входу 1 ПАК «Аист».

Программно-аппаратный комплекс «Колибри» (рис. 5.28) предназначен для проверки выполнения норм эффективности защиты речевой информации. Комплекс позволяет оценить возможности её утечки по акустическому и виброакустическому каналам, а также за счет эффекта акустоэлектрических преобразований в ВТСС и линиях ТСПИ. С помощью аппаратуры комплекса можно проводить:

- измерение акустического давления;
- измерение виброускорения;
- измерение уровней сигналов, образованных в результате проявления эффекта акустоэлектрических преобразований в линиях ТСПИ;
- расчёт показателей эффективности защиты выделенных помещений 1-й, 2-й и 3-й категорий.

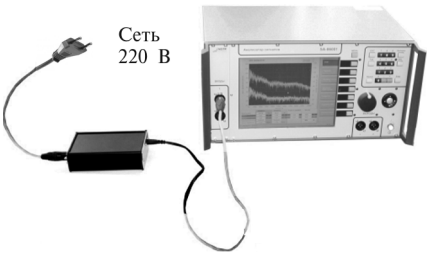


Рис. 5.27. Подключение комплекса «Аист» при исследовании цепи питания

Рис. 5.28. Программно-аппаратный комплекс «Колибри»

Комплекс «Колибри» создан на основе многофункционального концентратора-анализатора низкочастотных сигналов СКМ-8.

В базовый комплект поставки программно-аппаратного комплекса «Колибри» входят: многоканальный анализатор-концентратор сигналов СКМ-21.1; кабель подключения анализатора-концентратора СКМ-8 к USB порту ПЭВМ; измерительный микрофон МР201; микрофонный предусилитель КММ402; держатель для микрофона; измерительный акселерометр АР2037-100 (АР98-100); зарядное устройство; модуль дистанционного управления «Колибри -МДУ1»; дистанционно управляемый генератор шума «Колибри-АТ1» (встроен в монитор FOSTEX 6301B) с внешней антенной и пультом (брелоком) дистанционного управления; кабель подключения микрофона к анализатору-концентратору СКМ-8 (BNC–BNC); кабель подключения акселерометра к анализатору СКМ-8 (10-32–BNC); универсальный кабель-переходник LEMO-BNC для линейного канала анализатора-концентратора СКМ-8; гальванический контакт подключения несимметричных линий к линейному каналу анализатора-концентратора СКМ-8 (переходник BNC — гальванический контакт); гальванический контакт подключения симметричных линий к линейному входу анализатора-концентратора СКМ-8; Т-коннектор для подключения к разъему BNC; заглушка на разъем BNC сопротивлением 600 Ом; CD-диск с программным обеспечением СКМ-8 ПО (базовый комплект).

Комплекс работает в автономном, централизованном (по шине USB ПЭВМ) режиме. При этом с помощью комплекса можно успешно решать выполнять оценку:

- эффективности защиты речевой информации;
- параметров сигналов (октавный анализ; 1/3-октавный анализ);
- эффективности защиты речевой информации от утечки по акустическому и виброакустическому каналам (индекс артикуляции, отношение сигнал/шум, словесная разборчивость речи), по каналу АЭП (уровень сигнала, отношение сигнал/шум); при оценке

словесной разборчивости речи комплекс работает в двух режимах — ручном и автоматическом.

После рассмотрения характеристик основных комплексов остановимся на основных особенностях проведения специальных исследований в области акустики и вибраций. В действующих нормативных документах методика измерений защищённости построена на моделировании человеческой речи шумовым тест-сигналом с определённой огибающей спектра. Метод измерения основан на предварительной калибровке передающей части комплекса в условиях, которые определяются как свободное пространство. Затем откалиброванная таким образом передающая часть переносится в исследуемое помещение. В помещении выполняются уже измерения только результатов воздействия тест-сигнала, а уровень звукового давления исходного тест-сигнала принимается постоянным (измеренным при калибровке). Многочисленные экспериментальные работы позволили сделать вывод, что этот подход не даёт объективной картины защищённости конструкций ЗП. В зависимости от характеристик помещения и от размещения в нём акустического излучателя разница в итоговой оценке может достигать достаточно больших величин. При описании процесса калибровки указывается лишь то, что при её проведении достаточно разместить излучатель и микрофон в 1 м друг от друга, одновременно обеспечив расстояние не менее 1,5 м от любых конструкций. Других ограничений не приведено. Какие-либо иные характеристики помещения не приведены, как и условия и периодичность выполнения этой калибровки. Практическая проверка этой методической рекомендации показывает, что в зависимости от акустических характеристик помещения результат таких измерений (калибровки) при неизменной подводимой к излучателю мощности может отличаться на 6...15 дБ. Рассмотрим, какие факторы позволяют получить такие отличия.

При рассмотрении методов измерений в строительной акустике, предписываемых регламентирующими документами, наиболее близкими, совпадающими по физическому смыслу измерениями являются измерения звукоизоляции ограждающих конструкций в строительстве, регламентируемые ГОСТ 27926-87. В соответствии с этим стандартом выполняются измерения «на проход», со стороны конструкции, где размещён излучатель тест-сигнала, а затем с противоположной. Разность измеренных звуковых давлений и будет характеризовать звукоизоляцию. Кроме того, измерения выполняются на шумовом сигнале в третьоктавных (октавных) полосах. На этом сходство заканчивается. В ГОСТ 27926-87 строго регламентированы размеры смежных помещений (между которыми находится исследуемый образец конструкции), время реверберации в обоих смежных помещениях (раздел 3.1 «Требования к помещениям для испытаний ограждающих

конструкций в лабораторных условиях» и раздел 3.2 «Требования к помещениям для испытания внутренних ограждающих конструкций в натурных условиях»).

Последний параметр особенно важен, так как специально оговорено его минимальное значение и предписаны меры по обязательному выполнению этого требования. Обращаясь к физическим основам акустики, это должно интерпретироваться как условие, обеспечивающее диффузное акустическое поле в помещении высокого уровня звукового давления. В этом и только в этом случае можно утверждать, что на исследуемую конструкцию в любой её точке падает суммарная звуковая энергия приблизительно одинаковой величины.

Акустический излучатель должен устанавливаться не менее, чем в двух регламентированных точках. Уровень звукового давления в помещениях высокого и низкого уровней должен быть измерен не менее, чем в 6 точках (по три в каждом положении излучателя). В расчётные формулы входит и эквивалентное поглощение помещения низкого уровня.

Таким образом, описанная процедура калибровки передающей части комплекса не соответствует по ряду важнейших параметров условиям действующих ГОСТ и противоречит физическому смыслу. Кроме того, действующие методические указания предписывают два возможных варианта размещения акустического излучателя в исследуемом помещении и всегда на высоте 1,5 м от поверхности пола:

1) в точке постоянной локализации источника речевой информации (постоянное место докладчика, возможно — место руководителя);

2) при отсутствии постоянной локализации источника — в 1 м от исследуемой конструкции.

В отношении первого варианта особых претензий к такой рекомендации не возникает, действительно, при фиксированном размещении источника любые особенности помещения (путь звуковой волны, её отражения, поглощение и т. д.) по отношению к любой конструкции постоянны и входят некой константой, которая учитывается при измерениях в расчётные отношения. Однако оценка этим методом не предусматривает передвижений источника речевого сигнала вообще. Если источник (человек), произносящий нечто защищаемое, «прогуляется» по кабинету ближе к окну, звуковое давление опасного сигнала возрастёт и естественно может привести к превышению норм и, как следствие, к утечке информации.

Поэтому, как правило, в рабочих помещениях определить и предписать одно фиксированное место невозможно, следовательно, на практике чаще применяется второй вариант. При этом ограждающая конструкция с совершенно произвольными акустическими свойствами на расстоянии 1 м от излучателя будет вносить значительные

искажения в те цифры, которые были зафиксированы при начальной калибровке акустического излучателя.

Из-за этого точность измерений и повторяемость результатов при строгом выполнении положений методики будут составлять, ориентировочно, не лучше $\pm 10 \ldots 15$ дБ. Такая «девиация» результатов полностью исключает возможность нормального контроля правильности проведённых измерений и порождает многочисленные споры между исполнителями и контролирующими инстанциями.

Для исключения разброса результатов ведущими специалистами в области специсследований предлагается альтернативый вариант, по их мнению, позволяющий автоматически учесть все непредсказуемые характеристики исследуемого помещения. С этой целью предлагается несколько изменить метод измерений, а именно: предварительную калибровку заменить на измерение падающей на исследуемую конструкцию звуковой волны в каждой контрольной точке. То есть перейти на режим двухканального относительного измерения в режиме реального времени. Таким образом можно полностью исключить погрешности, вытекающие за счёт свойств конкретного помещения, как бы они не влияли на распределение звуковой энергии тест-сигнала в помещении в любой его точке. Потому что в каждой выбранной точке будет измерено звуковое давление, падающее именно на данный, контролируемый участок конструкции.

Экспериментальные проверки такого режима (метода) измерения позволили сделать вывод о высокой повторяемости результатов с возможной девиацией от измерения к измерению не более $1 \ldots 2$ дБ. При неизменности размещения элементов измерительного комплекса повторяемость в эксперименте достигала $\pm 0{,}3$ дБ несмотря на смещение положения двух операторов вблизи излучателя и первого микрофона. Чувствительность к размещению микрофона, т. е. изменение показаний при его сдвиге относительно установленного методикой положения (1,5 м от пола; 0,5 м от измеряемой конструкции; 1 м от акустического излучателя по оси излучения) в пределах смещений $5 \ldots 10$ см имеет те же величины.

Кроме того, при оценке таким методом любая ограждающая конструкция, в любой своей точке будет гарантированно защищена от утечки (по крайней мере, с точки зрения безусловного выполнения норматива на параметр защищённости).

Для реализации именно такого модифицированного метода измерения необходимо иметь двухканальную систему, которая выполняет измерения в первой и второй точках в едином измерительном цикле, одновременно учитывая в расчётах неидентичность амплитудно-частотных характеристик двух микрофонов.

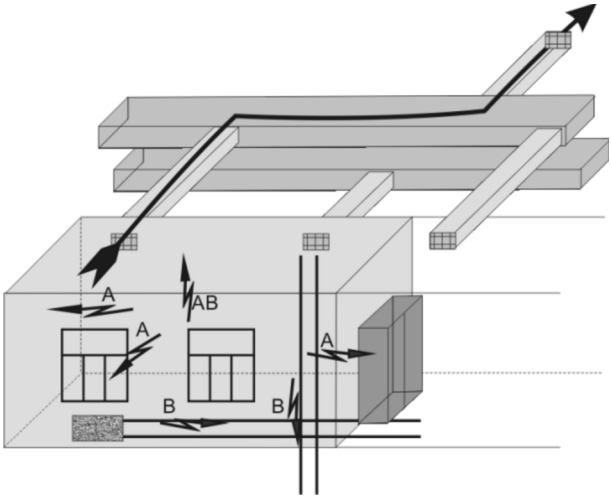


Рис. 5.29. Схема защищаемого помещения

Типовое защищаемое помещение показано на рис. 5.29. На рисунке приведен типовый набор элементов, образующих потенциальные каналы утечки акустической и вибрационной информации (дверные и оконные проемы, вентиляция, система отопления). Стрелками показаны некоторые из потенциальных направлений возможной утечки речевой информации. Стрелки с индексом «A» иллюстрируют акустические, а с индексом «B» — вибрационные каналы утечки.

В соответствии с этим основной задачей при проведении специсследования будет необходимость проведения измерений собственно ограждающих конструкций (стен, перекрытий потолка и пола) по акустическому каналу и по вибрационному, если такой канал оценивается. Для акустического замера элементы измерительного комплекса размещаются штатно — излучатель тест-сигнала (колонка) в 1,5 м от конструкции (по нормали к ней) на высоте 1,5 м от пола, первый микрофон в 0,5 м от ограждающей конструкции, второй за ней, также в 0,5 м от неё. Когда есть уверенность, что в ограждающей конструкции нет «слабых» мест, достаточно одного–двух замеров вдоль стены. Если есть подозрения на трещины, проходы (отверстия), неплотные (незаделанные) стыки отдельных панелей и т. д., необходимо увеличивать число контрольных точек. Минимальное расстояние между контрольными точками должно быть 1,5. . . 2 м.

На рис. 5.30 и 5.31 изображены основные варианты размещения элементов измерительной системы при измерениях основных ограждающих и инженерных конструкций.

При рассмотрении вариантов измерений следует иметь в виду,

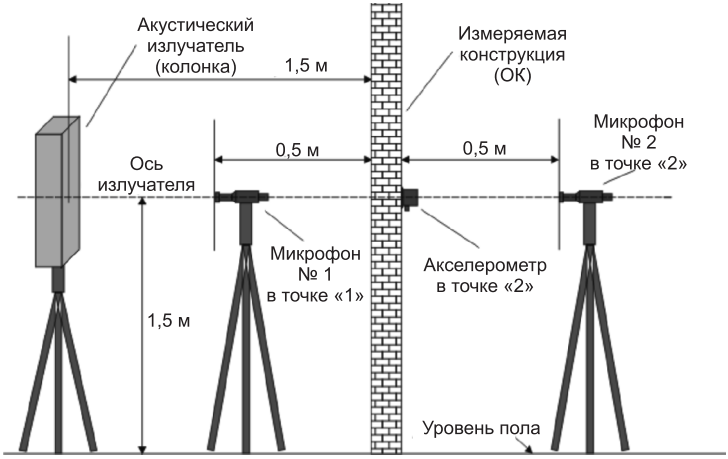


Рис. 5.30. Схема измерения стены (перегородки)

что при применении предложенной методики, в принципе, совершенно безразлично, где и как размещён акустический излучатель (это рассматривается как значительное положительное свойство метода). В любом случае измеряеся падающая на ограждающую конструкцию в конкретной точке звуковая волна. При этом важно, что измеряется

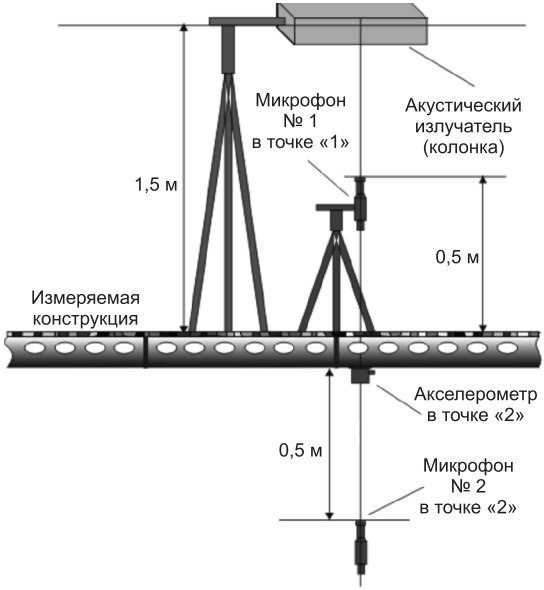


Рис. 5.31. Схема измерения перекрытия пола (акустика и вибрации)

падающая волна именно в конкретной точке. Если звуковое давление в точке «1» уменьшится, например, за счёт отодвигания излучателя, то ровно на ту же величину (точнее — весьма близкую) и с тем же знаком изменится и звуковое давление в точке «2». При данном методе расчёта результаты не изменятся принципиально. В связи с этим в примерах точные параметры размещения акустического излучателя приведены только для буквального выполнения требований утверждённой методики.

Аналогично выполняются измерения по вибрационному каналу, в том числе и при оценке эффективности средств активной защиты. В последнем случае надо иметь в виду, что необходимо контролировать отдельно каждый элемент ограждающей конструкции, например каждую отдельную плиту перекрытия пола (потолка) или отдельные конструкции стен (например, отдельные бетонные плиты). Размещая акселерометр, обязательно необходимо обратить внимание на то, что при любых вибрационных измерениях акселерометр должен размещаться на поверхности основной несущей конструкции (бетоне, кирпиче и т. д.). Измерения при размещении акселерометра на рыхлой штукатурке, побелке, обоях, линолеуме и т. д. дают недостоверные результаты и недопустимы.

Приведенные схемы являются основными, типичными. Выбор размещения элементов измерительной системы в каждой конкретной точке измерения — дело оператора. При этом данный выбор должен обосновываться и излагаться в соответствующем разделе протокола.

Некоторые особенности есть при измерениях перекрытий пола и потолка. Излучатель размещается штатно, над полом ЗП, а микрофоны № 1 и № 2 по обе стороны измеряемой ограждающей конструкции, как показано на схеме. Во время измерений перекрытия потолка микрофон № 1 размещается под потолком, на расстоянии 0,5 м от него и развернут вертикально вниз. Микрофон № 2 — над полом в выше расположенном помещении, также на высоте 0,5 м, ориентирован по нормали к плоскости пола и направлен вниз. Если в выделенном помещении имеется фальш-потолок, то в любом случае микрофон размещается в 0,5 м от потолка помещения (подвесного, подшивного или основного перекрытия). Следует отметить, что вибрационный канал утечки следует рассматривать (кроме окон), чаще всего, «на границе КЗ», так как внутри КЗ технический перехват, как правило, исключен организационными мерами, в обязательном порядке обеспечиваемыми заказчиком.

Схема расположения элементов измерительной системы при измерениях защищенности дверей (рис. 5.32) понятна без особых комментарий, так как является всего лишь повторением схемы, приведенной на рис. 5.30. Необходимо только проследить, чтобы все двери

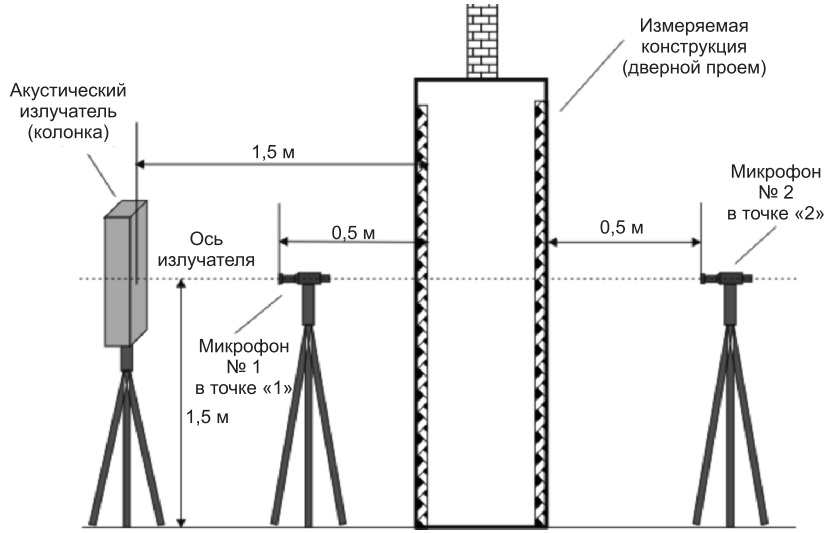


Рис. 5.32. Схема измерения двойного дверного проема

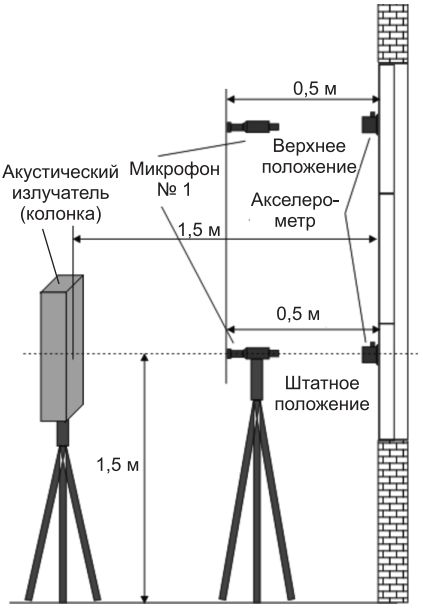


Рис. 5.33. Схема измерения на окне

(полотна дверей) были плотно закрыты. Аналогичная схема применяется и при измерении звукоизоляции оконных блоков (рис. 5.33).

Измерения защищенности по вибрационному каналу (при помощи оптико-электронной (лазерной) аппаратуры дистанционного прослушивания речи) на остеклении окон имеют некоторые особенности.

Как правило, часть створок окон оказывается заметно выше осевой линии излучателя, которая по методике должна быть расположена на высоте 1,5 м от пола. Если провести контрольные измерения уровня звукового давления падающей волны «внизу» и «наверху» на одинаковом штатном удалении от плоскости стекла 0,5 м, то, за редким исключением, «наверху» значения окажутся на 3...8 дБ меньше, чем «внизу». При расчете соотношений сигнал/шум (или значений «W»)

вблизи критических (нормативных) значений это очень большая разница. Поэтому, если при нижнем, «штатном» размещении микрофона и акселерометре вверху створки расчеты показали величины, близкие к нормированным, необходимо повторить измерения, разместив микрофон № 1 (по высоте) напротив центров соответствующих фрамуг. Естественно, эта ситуация и действия оператора должны быть отражены в протоколе. Данная рекомендация может показаться искусственной, вряд ли «некий» источник речевой информации будет подниматься выше типовых 1,5 м от пола, т. е. вряд ли звуковое давление, воздействующее на верхнюю створку возрастёт.

В настоящее время получение результатов, удовлетворяющих требованиям нормативных документов, еще не гарантирует защиту от утечки речевой информации через оптико-электронный (лазерный) канал. Для оценки реальной степени защиты от утечки информации по данному каналу российскими специалистами разработано устройство оценки защищенности помещений по лазерному каналу СТБ-171. Данное устройство (рис. 5.34) предназначено для оценки защищенности помещений от утечки речевой информации при использовании противником электронноoптических лазерных средств дистанционного съема информации.

Конструктивно устройство СТБ-171 выполнено в моностатическом корпусе с совмещенными осями передатчика и приемника. Принцип действия устройства СТБ-171 основан на регистрации зондирующих сигналов, отраженных от поверхностей, в которых под действием речевого сигнала возникают упругие колебания.

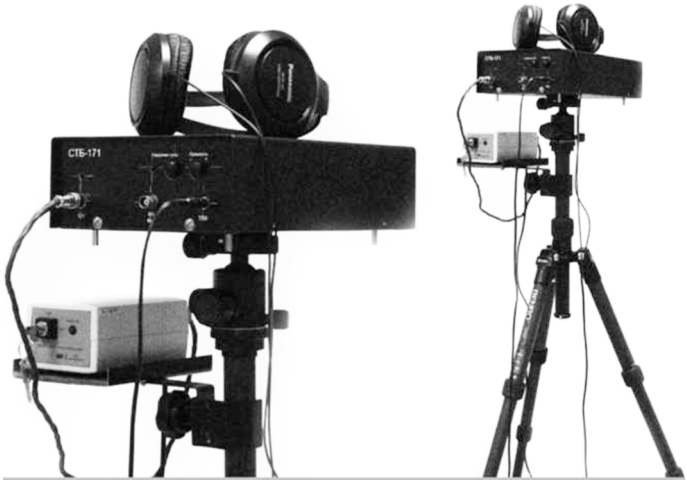


Рис. 5.34. Устройство оценки защищенности помещений по лазерному каналу

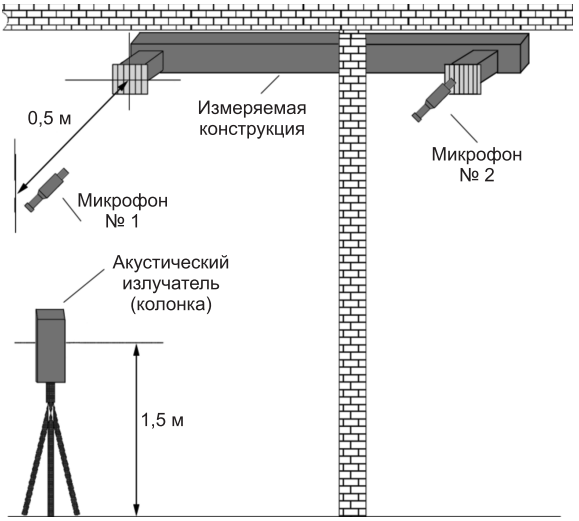


Рис. 5.35. Схема измерения в системе вентиляции

Устройство имеет следующие основные характеристики: мощность источника лазерного излучения 200 мВт; источник лазерного излучения имеет длину волны 1,06 мкм; в устройстве предусмотрена возможность подключения анализирующей, регистрирующей аппаратуры и средств прослушивания выходного низкочастотного сигнала (головных телефонов с сопротивлением не менее 15 Ом); возможность размещения на штативе, позволяет изменять направление излучения в двух плоскостях; при проведении измерений на реальных предметах (шторы, жалюзи и т. п.) рекомендуемая дальность от 5 до 20 м, при этом диаметр лазерного луча на расстоянии 20 м равен 5 см.

Полученные результаты оценки степени защищенности по каналу утечки речевой информации по оптико-электронному (лазерному) каналу позволить выбрать необходимый комплекс мер защиты.

Измерения в системе вентиляции (рис. 5.35) должны проводиться следующим образом. Излучатель размещается вблизи входного окна вентиляции на высоте 1,5 м от пола, строго выдерживать расстояние в 1,5 м, например, от стены нет необходимости. Микрофон № 1 размещается в 0,5 м по нормали от плоскости вентиляционного окна (решетки) и ориентируется по нормали к решетке. Второй микрофон размещается в *плоскости* ближайшего (по ходу короба вентиляции) вентиляционного окна, а не в 0,5 м от него. Данная рекомендация основывается на том, что если говорить о непреднамеренном прослушивании именно в этом случае, то постороннее ухо с той же вероятностью может оказаться в плоскости решетки, как и в 0,5 м от нее.

В этом случае мы имеем дело не с плоской, а сферической звуковой волной, и спадание уровня звукового давления с удалением происходит пропорционально третьей степени расстояния. Соответственно оценка защищенности в плоскости решетки и в 0,5 м от нее будет отличаться многократно.

Уровень тест-сигнала (громкость звучания измерительной колонки) устанавливается в зависимости от решаемой задачи. Общая рекомендация заключается в том, чтобы уровень измеряемого сигнала «на» или «за» исследуемой конструкцией не менее чем на 10 дБ превышал уровни фоновых шумов.

Обычно при измерениях на окнах для одиночных стекол достаточно звукового давления тестового сигнала около 60...65 дБ, для стеклопакетов — 70...80 дБ. При оценке дверных проемов общего типа, даже двойных (но выполненных без применения специальных мер акустической защиты), достаточно уровня 70...75 дБ. Для дверей с усиленной защитой — до 90 дБ. Для капитальных перегородок (стен) уровень тест-сигнала приходится поднимать до допустимого максимума. При этом допустимо повышать или понижать уровень тест-сигнала в одной из отдельно взятых полос, т. е. формировать неплоскую амплитудно-частотную характеристику (это возможно только при использовании соответствующего источника тест-сигнала с эквалайзером).

Вопрос об оценке уровней фоновых шумов целесообразно рассмотреть отдельно. Хотя рассматривать данный вопрос имеет смысл только в привязке к конкретному средству измерения. В подавляющем большинстве случаев уровень акустических фоновых шумов не менее 30 дБ, а для вибраций — не менее 15...25 дБ, что должно учитываться при выборе измерительной техники. В ограниченном числе случаев, например при измерениях в ночное время на капитальных строительных конструкциях (особенно в загородной зоне) по вибрационному каналу или в очень тщательно звукоизолированных помещениях по акустическому каналу, реальный уровень фоновых значений виброускорения или звукового давления может снижаться до значений 4...6 дБ. При этом необходимо применять другие моделей акселерометров (микрофонов) с меньшим уровнем собственных шумов.

Оценку защищенности по вибрационному каналу, на трубах (стояках) отопления (рис. 5.36) рекомендуется производить следующим образом. Акустический излучатель необходимо расположить в 1,5 м от плоскости батареи отопления на обычной высоте от пола. Микрофон № 1 располагается напротив центра батареи в 0,5 м от ее плоскости, направленной к излучателю. Акселерометр крепится на трубу (стояк) в 10...15 см от места выхода трубы из выделенного помещения(от стены, потолка, пола). Такое размещение применяется в

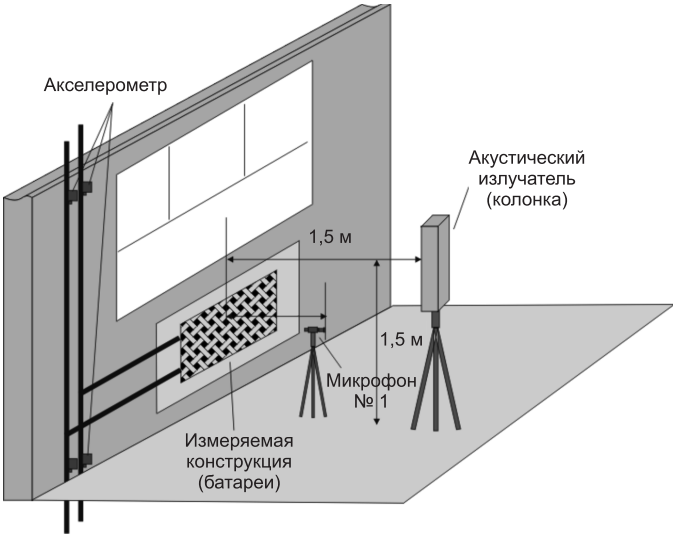


Рис. 5.36. Схема измерений на батарее отопления

том случае, когда границей контролируемой зоны для данного канала являются ограждающие конструкции помещения. Если же граница контролируемой зоны проходит в точке выхода основных трубопроводов из здания, то прямой замер защищенности, как правило, невозможен из-за значительного затухания вибрационного тест-сигнала на пути от защищаемого помещения до точки измерения акселерометром. В этом случае надо размещать акселерометр ближе к выделенному помещению, там, где тест-сигнал имеет измеряемую величину, а результаты измерения позволяют сделать вывод о выполнении условий защищенности (соседнее помещение, через помещение, ближайший этаж в сторону границы контролируемой зоны и т. д.). На основании такого измерения можно сказать, что на границе контролируемой зоны затухание много больше, следовательно, условия защищенности выполняются.

Второй метод состоит в измерении реального затухания в канале утечки. Это позволяет оценить степень защищенности при очень значительных затуханиях в канале. Его физическая суть заключается в создании в канале утечки столь «большого» тест-сигнала, что его удается зафиксировать (измерить) над уровнем шумов на дальнем конце канала. Для создания такого высокого по величине сигнала его необходимо «вводить» в канал не «озвучиванием», которое имеет огромные потери при переходе из воздушной среды в твердое тело, а непосредственно, с помощью соответствующего вибровозбудителя. Для этой цели подходит преобразователь TRN2000 (а также КВП-2,

КВП-6, КВП-8), который при подключении к генератору тест-сигнала легко позволяет создать в трубопроводе тест-сигнал с уровнем 120...130 дБ (относительно 10^{-6} м/с^2) при том, что с помощью акустического излучателя с уровнем звукового давления примерно 100 дБ в том же трубопроводе не удается создать вибрационный сигнал (виброускорение) большее 75...80 дБ.

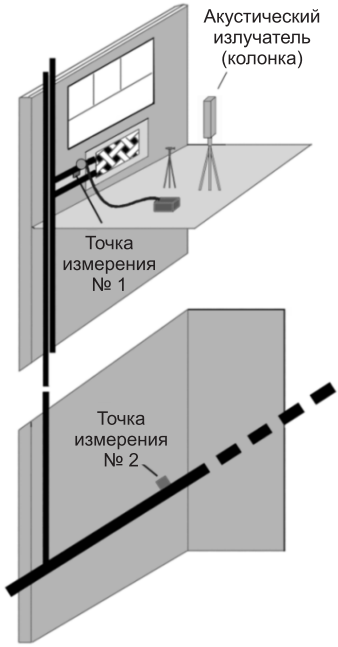


Рис. 5.37. Схема измерения в вибрационном канале с учетом реального затухания

Созданный уровень тест-сигнала необходимо измерить во всех пяти октавных полосах в точке, находящейся от возбуждающего преобразователя не далее, чем на 10...15 см. Второй замер выполняется на границе контролируемой зоны (рис. 5.37). Разность между значениями тест-сигнала в этих двух точках и есть реальное затухание в канале. Обычно в реальных условиях во второй точке тест-сигнал удается измерить над уровнем шумов при расстояниях (по погонной длине трубопроводов) не менее 50...100 м (в основном в зависимости от уровня сторонних шумов во второй точке).

Если тест-сигнал не выявляется, можно первую точку (точку ввода тест-сигнала) приблизить к границе контролируемой зоны до появления тест-сигнала. Если удается измерить реальное затухание не во всех пяти октавных полосах (например, в трех иди четырех), то можно рекомендовать «распространить» минимальное из полученных затуханий на те октавы, в которых его измерить не удалось. Поэтому оператору необходимо обосновать такое решение.

После этого производится измерение тест-сигнала в системе отопления (колонка в 1,5 м от батареи, микрофон в 0,5 м, акселерометр на границе ВП). Полученные в обоих измерениях результаты обрабатываются следующим образом.

Как правило, значения во второй точке (при измерении затухания) мало отличаются от уровня сторонних шумов (т. е. измеряется не «чистый» тест-сигнал, а его смесь со сторонними шумами). Поэтому во второй точке необходимо измерять раздельно уровни помех (при выключенном источнике тест-сигнала) и смесь тест-сигнала с шумами (источник включен). Далее реальное затухание в каждой ок-

Таблица 5.2

$F_{\text{цент}}$, Гц	V_{1i}, дБ	$V_{2i,\text{с+ш}}$, дБ	$V_{2i,\text{ш}}$, дБ	ΔV_i
250	113,7	28,3	28,4	—
500	112,9	24,2	23	94,87
1000	107	24,3	23	88,57
2000	112,1	27,1	22	86,60
4000	109,3	25,3	24	89,87

тавной полосе вычисляется по формуле

$$\Delta V_i = V_{1i} - 20\log_{10}\sqrt{10^{V_{2i,\text{с+ш}}/10} - 10^{V_{2i,\text{ш}}/10}},$$

где в i-й октавной полосе ΔV_i — реальное затухание, дБ; V_{1i} — значение тест-сигнала в точке *1* (рядом с точкой его ввода), дБ; $V_{2i,\text{с+ш}}$ — значение тест-сигнала в точке *2* (на границе КЗ), дБ; $V_{2i,\text{ш}}$ — значение фонового шума в точке *2* (на границе КЗ), дБ.

При реальном замере будут получены примерно такие данные, которые приведены в табл. 5.2. Из таблицы видно, что реальные затухания для данного примера весьма значительны. В октавной полосе с центральной частотой 250 Гц затухание не могло быть рассчитано, поскольку тест-сигнал не выявлен над уровнем шумов.

Таким образом, вычисляются реальные затухания в октавных полосах. Далее, для упрощения расчетов, примем, что минимальное из полученных значений используется при расчете защищенности по всем октавам.

Замер опасного сигнала в батарее, т. е. ее «озвучивание», описанное выше, дает типовые значения, приведенные в табл. 5.3.

Для выполнения стандартного расчета защищенности необходимо иметь значения тест-сигнала во второй точке. Покажем, как можно рассчитать эти значения с учетом измеренного реального затухания. Рассуждать в этом случае необходимо следующим образом:

1. Предположим, что сторонние шумы на границе контролируемой зоны такие же, как в точке *1*. На самом деле они всегда больше

Таблица 5.3

$F_{\text{цент}}$, Гц	L_{ci}, дБ	$V_{(\text{с+ш})i}$, дБ	$\Delta V_{\text{ш}i}$, дБ
250	97,6	76,2	28,4
500	96,3	72,4	23
1000	98,4	73,62	23
2000	98,5	70,9	22
4000	99	67,7	24

$F_{\text{цент}}$ — центральная частота октавной полосы; L_{ci} — уровень звукового давления, развиваемый излучателем («озвучка»); $V_{(\text{с+ш})i}$ — смесь сигнала и шума, возникающая в трубе при воздействии тест-сигнала; $\Delta V_{\text{ш}i}$ — уровень сторонних шумов в трубе.

Таблица 5.4

$F_{\text{цент}}$, Гц	$\Delta V_{(\text{с+ш})i}$, дБ	ΔV_i, дБ, минимальное	$V_{\text{ш}i}$, дБ	$\Delta V_{(\text{с+ш})i}$, дБ, реальное
250	76,2	86	28,4	28,4007
500	72,4	86	23	23,0010
1000	73,62	86	23	23,0013
2000	70,9	86	22	22,0008
4000	67,7	86	24	24,0003

(при работающей системе отопления в этой точке вода в трубопроводе заметно шумит). При неработающей системе шумы в обеих точках примерно равны. Следовательно, такое предположение может лишь ужесточить условия защищенности и потому допустимо.

2. Рассчитаем, что произойдет с шумами в каждой октавной полосе, если к ним прибавиться тест-сигнал в точке *1*, уменьшенный на реальное минимальное затухание. Вычислим значение тест-сигнала в точке *2*, вызванного акустическим воздействием в точке *1*. Получаем

$$\Delta V_{(c+\text{ш})i\,\text{реал}} = 20\log_{10}\sqrt{10^{V_{1i}/10} + 10^{(V_{(c+\text{ш})i}-\Delta V_{i,\min})/10}}.$$

Вычислим по приведенной формуле значения тест-сигнала в точке *2*, предполагая, что реальное минимальное затухание по всем октавам не менее 86 дБ. Полученные значения приведены в табл. 5.4. Результаты расчета позволяют сделать вывод, о том что вычисленные значения тест-сигнала в точке *2* отличаются от шумов только в третьем-четвертом знаке после запятой. Измерить такие сигналы существующими средствами «напрямую» невозможно.

Подставив полученные значения в стандартный расчет параметров защищенности по НМД АРР и предполагая, что значения сигнала САЗ (V_{mi}), при отсутствии системы зашумления равны шумам, получим данные, которые приведены в табл. 5.5. Некоторые промежуточные данные расчета из-за недостатка места опущены.

Таким образом, мы видим, что в данном случае (как это реально и бывает) требуемые соотношения сигнал/шум выполняются в каждой октавной полосе с огромным запасом (несмотря на такие «ужесточающие» допущения при расчете).

Метод учета реального затухания может быть применен и в акустических замерах. Для этого нужно использовать мощный малогабаритный излучатель, который можно ввести, например, в воздуховод. Все остальное выполняется аналогичным образом. Следовательно, проведенные измерения и полученные результаты позволяют рассмотреть и возможные варианты активной защиты.

Рассмотрим **основные рекомендации по размещению и оптимизации системы активной защиты**. В настоящее время применение

$F_{\text{цент}}$, Гц	L_{ci}, дБ	$V_{(\text{с+ш})i}$, дБ	$V_{\text{ш}i}$, дБ	V_{mi}, дБ	$L_{\text{н}i}$, дБ	$C_{L\text{т}}$, дБ	V_{ci}, дБ
250	97,6	28,4	28,4	28,4	66	31,6	−9,80
500	96,3	23,0	23	23	66	30,3	−13,60
1000	98,4	23,0	23	23	61	37,4	−12,38
2000	98,5	22,0	22	22	56	42,5	−15,10
4000	99	24,0	24	24	53	46	−18,30

системы активной защиты для обеспечения защищенности по акустическим и вибрационным каналам достаточно распространено. При этом данный способ, достаточно простой и дешевый, тоже имеет свои недостатки.

Одним из основных недостатков является увеличение уровня паразитного шума в защищаемом помещении, причем не только за счет самого акустического зашумления, сколько за счет тех паразитных акустических шумов, которые появляются на защищенных вибропреобразователями стеках окон. К сожалению, стекла можно рассматривать как мембраны достаточно большой площади. Поэтому при установке вибровозбудителей зашумления они достаточно сильно шумят, заметно больше, чем стены, трубы и т. д. Именно поэтому рациональное размещение датчиков на стеклах, тщательная настройка амплитудно-частотных характеристик источника шумового сигнала являются наиболее важными задачами для специалиста в этой области. При этом необходимо иметь в виду, что вибровозбудители необходимо размещать *только на стеклах*. Все известные нам попытки «зашумлять» рамы, оконные коробки приводят к недопустимому уровню акустических шумов при выполнении норм защищенности. К таким же малоприятным «последствиям» приводит размещение в межстекольном пространстве акустических колонок.

В среднем, на обычном одиночном стекле оптимально размещать на 1 м^2 стекла два вибровозбудителя, при остеклении стеклопакетом — до 4. Увеличивается и количество вибровозбудителей на узких, вытянутых створках. Дать рекомендации на все случаи практически невозможно, многое решается «на месте», исходя из опыта, а чаще на основании пробных замеров.

Серьезная оптимизация, при которой производится индивидуальная настройка каждой створки, возможна только при использовании генераторов системы активной защиты, имеющих полосовые регуляторы АЧХ. При большом числе отдельных створок (свыше 10), особенно различной формы, настоятельно рекомендуется применение систем защиты модульного типа, с большим числом независимо регулируемых каналов.

Достаточно сложен и вопрос выбора контрольных точек на плос-

Таблица 5.5

$V_{ci} - V_{Ст}$, дБ	E_i, дБ	Вып. нормы в полосе	R	W
−41,40	−69,80	Да	$2{,}6 \cdot 10^{-9}$	$3{,}1 \cdot 10^{-10}$
−43,90	−66,90	Да		
−49,78	−72,78	Да		
−57,60	−79,60	Да		
−64,30	−88,30	Да		

кости стекла при проведении измерений и оценке эффективности системы активной защиты. Оценки в одной–трёх точках бывает абсолютно недостаточно.

На рис. 5.38 показаны рекомендованное распределение вибровозбудителей и минимально необходимое количество контрольных точек на стеклах различной формы.

Данные рекомендации не исключают зачастую значительно большего числа контрольных точек, которые могут отстоять друг от друга не более чем на 5...6 см. Это бывает необходимым на сложных стеклопакетах в выделенных помещениях высокой категории. В настоящее время руководящими документами строго не определено, какая из нескольких имеющихся поверхностей остекления наиболее опасна для вибрационного канала при применении лазерных средств дистанционного съема информации. Указывается лишь, что в отношении внутренних поверхностей рассматривается вариант зеркального отражения, а в отношении внешней поверхности — отражение диффузное. В связи с этим, строго говоря, опасны все поверхности, а следовательно, должна оцениваться защищенность для каждой из них (рис. 5.39).

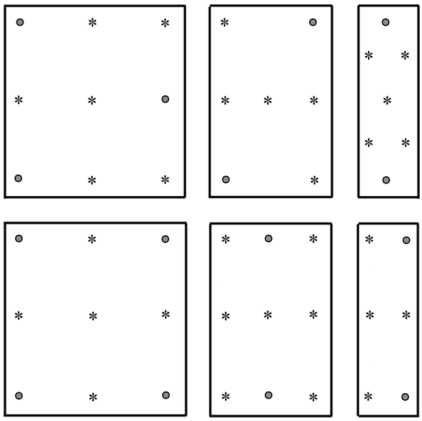


Рис. 5.38. Рекомендуемое размещение контрольных точек на стеклах: • — вибровозбудители САЗ; ∗ — контрольные точки

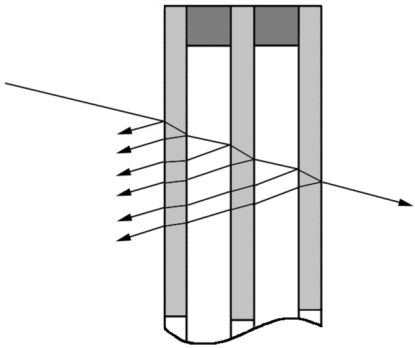


Рис. 5.39. Зеркальное отражение лазерного луча от многослойного остекления

Каждый из отраженных лучей может быть раздельно «принят» и обработан соответствующими техническими средствами. Априори, можно утверждать, что отраженный луч уменьшается по энергии при отражении от более далекой поверхности, но одновременно он модулирован вибрационным сигналом большей амплитуды. Поэтому вопрос о том, какой из них более опасен, требует специального изучения.

При рассмотрении вопросов оценки вибрационной защиты остекления защищаемых помещений от возможного съема информации по оптоволоконному (лазерному) каналу опытным путем был получен результат, который позволил сделать следующие выводы:

- прежде всего необходимо пересмотреть требования нормативных документов в области защиты речевой информации по оптоволоконному (лазерному) каналу;
- применение для защиты от утечки речевой информации по данному каналу только виброизлучателей не обеспечивает необходимый уровень защиты, даже при работе их на максимальной мощности;
- для обеспечения необходимого уровня защиты наиболее целесообразно использование комплексных мер защиты, а именно виброизлучатели и пассивные меры защиты (использование штор из материала, прошедшего специальную проверку).

Наиболее сложный для обеспечения защиты вариант, когда датчики зашумления размещаются на внутренней поверхности внутреннего остекления, а оценку защищенности необходимо, по требованиям документов, производить на самой наружной. В этом случае особенно сложно обеспечить приемлемый уровень побочных шумов.

В документах указан предельный угол (по отношению к нормали), в котором рассматривается падение лазерного луча на поверхность. Следует учитывать, что при угле падения около 57° на границе воздуха и обычного стекла луч претерпевает полное отражение, т. е. отраженная энергия максимальна. Правда, при этом он полностью отражается от первой же поверхности (самой внешней) и не проникает дальше.

Особенности применения системы активной защиты. «Зашумление» ограждающих конструкций не вызывает каких-либо принципиальных сложностей. Следует только не забывать, что если ограждающие конструкции состоят из отдельных элементов (например, бетонных панелей, плит), то, как правило, необходимо устанавливать вибровозбудители на *каждой* из них. Легкие перегородки, выполненные из гипсокартона, ДСП, ДВП и аналогичных материалов обычно «зашумить» не удается. В таких материалах сложно закрепить преобразователь и вибрационные колебания в них распространяются плохо.

При размере стёкол более 2×2 м и/или толщинах стёкол свыше 6 мм количество и размещение преобразователей должно выбираться

экспериментально. Ориентировочные варианты размещения преобразователей на остеклении приведены на рис. 5.40.

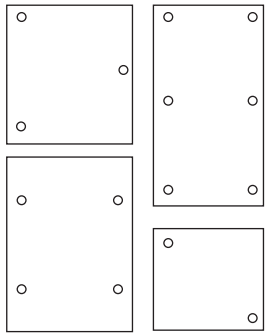


Рис. 5.40. Варианты размещения преобразователей на остеклении

При размещении на стекле более одного вибровозбудителя рекомендуется запитывать их от разных каналов системы зашумления. На одном стекле площадью до 1,7×1,5 м допускается подключение датчиков к двум каналам «через один». На больших площадях стёкол необходимо использовать три–четыре канала и т. д. При нарушении данного правила за счёт интерференции вибрационных синфазных колебаний, возбуждаемых в нескольких точках, как правило, возникают локальные зоны площадью примерно 20...40 см^2, в которых амплитуда вибраций резко снижена и условия защищённости не выполняется. Поиск таких зон весьма трудоёмок (приходится размещать десятки контрольных точек с шагом до 30 мм), а для их «закрытия» увеличить мощность подводимых к преобразователям сигналов. Это вызывает соответствующее повышение уровня паразитных акустических шумов.

Для обеспечения оптимальной защищённости остекления окон рекомендуется размещать вибровозбудители по образующей створке окна на расстоянии не менее 70 мм от обреза рамы и на расстояниях от вибровозбудителя до вибровозбудителя для внутреннего остекления одиночным стеклом (при его толщине 3...6 мм) не более 80 см, для наружного остекления одиночным стеклом (при его толщине 3...6 мм) — не более 1,3 м при расстоянии между стёклами более 80 мм и отсутствии щелей и неплотностей прилегания внутренних рам. Для внутреннего или единственного остекления одно- или двухкамерным стеклопакетом с толщиною стёкол 3...5 мм — не более 50 см. Для наружного (при расстоянии между стёклами не менее 80 мм и отсутствии щелей и неплотностей прилегания внутренних рам) остекления одно- и двухкамерным стеклопакетом с толщиною стёкол 3...5 мм — не более 80 см.

Вибровозбудители ПИ-45, КВП-7 и ПЭД-6 (или аналогичные) на остекление окон крепятся методом наклеивания. Обе склеиваемые поверхности в процессе их подготовки должны быть полностью свободны от любых покрытий и загрязнений. Очистка поверхностей выполняется в 3–4 этапа промывкой поверхностей растворителями (обезвоженный спиртобензин, толуол, «649», «647» или аналогичными) и сухой протиркой гигроскопичной стерильной ватой. При выполнении этой процедуры соблюдать осторожность, чтобы не повредить пьезоэлемент под мембраной вибровозбудителей.

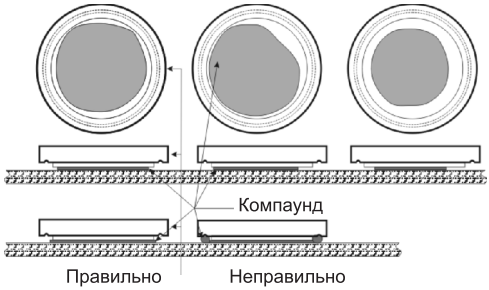


Рис. 5.41. Крепление преобразователей на стекло

Плёнка компаунда должна обладать достаточной механической жёсткостью, минимально возможной толщиной и высокой степенью адгезии к металлу и стеклу в течение всего срока эксплуатации при условии воздействия ультрафиолетового излучения и значительных перепадов температур. Особенно внимательно следует относиться к количеству компаунда, наносимому на склеиваемые поверхности. Плёнка компаунда должна быть сплошной (без разрывов и пузырьков), занимать не менее 90 % площади мембраны датчика и быть симметрично расположенной относительно центра датчика. Допускается незначительное выступание компаунда за пределы мембраны без склеивания стекла и любых участков корпуса датчика за пределами мембраны (рис. 5.41).

Для быстрой и надежной установки на стекло фиксатора типа 4м или изделий ПИ-45, ПИ-3М, СП-45М и СП-3Б лучше всего использовать специальный УФ отверждаемый клей и специальные УФ осветители в следующем порядке. Определяется место монтажа излучателя (фиксатора). Затем с помощью наждачной бумаги поверхности стекла в месте крепления излучателя придаётся шероховатость до сплошной потери прозрачности. Подготовленная поверхность стекла и приклеиваемая (пластмассовая) поверхность излучателя тщательно протирается тканью, обильно смоченной растворителем. Остатки растворителя должны улетучиться, после этого равномерно тонким слоем нанести УФ клей на склеиваемые поверхности. Затем приложить и прижать излучатель приклеиваемой поверхностью к стеклу. Накрыть излучатель УФ лампой (рис. 5.42) и нажать кнопку на корпусе лампы. После звукового сигнала снять УФ лампу. Излучатель готов к работе (если приклеивался фиксатор 4м, то необходимо аккуратно накрутить на него излучатель).

Рис. 5.42. Ультрафиолетовая лампа

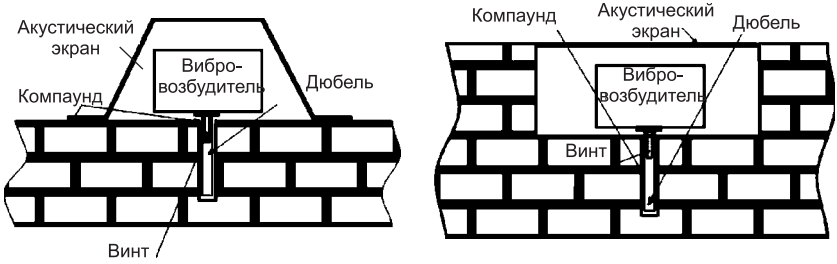


Рис. 5.43. Крепление вибровозбудителей на ограждающих конструкциях

Вибровозбудители ВД-45, ВИ-45, КВП-2 на ограничивающие конструкции ЗП устанавливаются при помощи имеющегося на их дне винта. Винт ввинчивается в металлический дюбель (входит в комплект поставки преобразователя), вклеиваемого эпоксидным компаундом в отверстие диаметром 8 мм, высверливаемое в конструкции (бетон, кирпич, камень и т. д.). При вклеивании внешний торец дюбеля должен выступать над плоскостью конструкции настолько, чтобы обеспечить отсутствие касания дна преобразователя к защищаемой конструкции в любой точке, кроме крепёжного винта (рис. 5.43).

Для снижения уровня паразитного акустического шума вибровозбудитель зачастую закрывается акустическим экраном. Экран устанавливается над вибровозбудителем и приклеивается к строительной конструкции с помощью любого строительного герметика таким образом, чтобы корпус вибровозбудителя не соприкасался с внутренней поверхностью экрана и отсутствовали щели между экраном и строительной конструкцией, а также в местах выхода кабеля.

Крепление вибровозбудителей может быть выполнено как открыто, так и скрытно (заглублено в конструкцию).

Вибровозбудители на ограничивающие конструкции ЗП устанавливаются в соответствии с техническим описанием и набором крепежных элементов. Наклейку выполняют аналогично наклейке на остекление.

Различные трубопроводы (отопление, водоснабжение, канализация и т. д.) «зашумляются» без проблем. Если они образуют связанную (в пределах выделенного помещения) систему, то зачастую вполне достаточно одного вибровозбудителя на всю систему. При этом его рекомендуется устанавливать приблизительно посередине этой системы, а контрольные точки для оценки эффективности выбирать вблизи выходов труб из выделенного помещения.

Вибровозбудители на трубопроводы различных инженерных систем (рис. 5.44) устанавливаются при помощи вспомогательных хомутов.

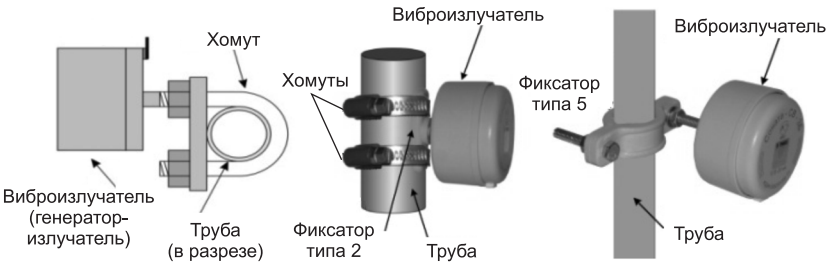


Рис. 5.44. Крепление преобразователей на трубопроводы

При защите дверных проемов, как правило, колонку системы активной защиты размещают в тамбуре двойной двери. Однако почти во всех случаях намного эффективнее размещать ее у косяка наружной (по отношению к защищаемому помещению) двери. В этом случае «зашумляется» опасный сигнал, ослабленный двумя дверьми, поэтому и сигнал системы активной защиты может быть намного слабее. В обратную сторону необходимый для обеспечения защиты уровень шума также ослабляется двумя дверями, чем достигается наиболее комфортные условия непосредственно в ЗП.

При отсутствии в конструкции двери порога независимо от площади проёма рекомендуется установка не менее 4-х излучателей на уровнях 1,5 и 0,5 м от уровня пола (рис. 5.45). Акустические излучатели могут размещаться как открыто, на плоскости ограждающей конструкции, так и полускрыто, в нишах стен, закрытых декоративными решётками и затянутых радиотканью.

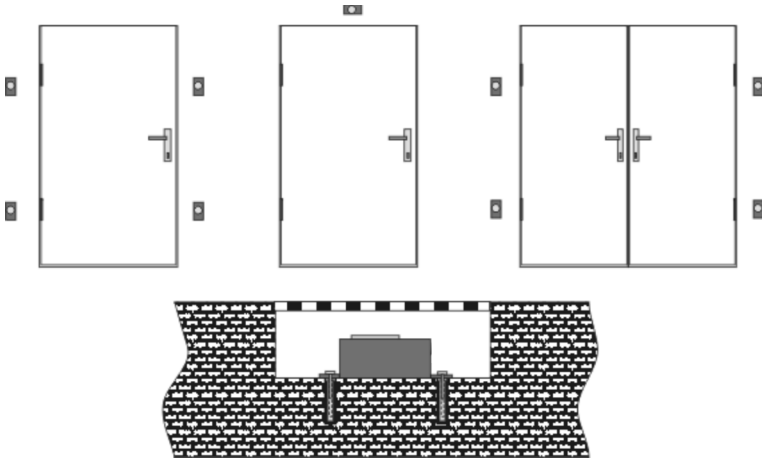


Рис. 5.45. Варианты размещения акустических излучателей для защиты дверного проёма

Акустическое зашумление бывает необходимым, в основном, при защите дверных проемов и систем вентиляции.

При защите систем вентиляции наилучшим местом размещения колонки системы активной защиты является короб (канал) вентиляции на расстоянии не менее 1,5 м в глубину от плоскости его выхода в ЗП. При таком размещении шум колонки не слышен в выделенном помещении, а защищенность достигается при невысоких уровнях громкости колонки.

Очень эффективным является размещение колонки в отдельном кожухе, «пристыкованном» к коробу вентиляции в том месте, где от него выполнен отвод в защищаемое помещение. Естественно, в стенке короба, там, где закреплен кожух с колонкой, должны быть проделаны отверстия для прохода звука. При таком размещении колонку легко извлечь для профилактического ремонта, очистки от пыли, при этом она не уменьшает своими габаритами сечение вентиляционного канала и не мешает нормальному воздухообмену.

Остальные, достаточно многочисленные варианты размещения вибровозбудителей и колонок системы активной защиты необходимо рассматривать для конкретных условий. В любом случае необходимо обеспечивать выполнение норм защищенности и принимать все меры к тому, чтобы это не мешало нормальной работе в защищаемом помещении.

5.2.5. Специальные исследования в области акустоэлектрических преобразований (СИ АЭП)

Основное содержание работ. Так же, как и при специальных исследованиях в области акустики и вибраций, рассмотрим основное содержание работ для этого вида СИ применительно к структуре рекомендуемого протокола измерений. В отношении разнообразных ТС, попадающих по СИ АЭП, могут проводиться как стендовые, так и объектовые СИ. Отметим, что стендовые СИ, как правило, можно выполнить с более высоким качеством, особенно если стенд размещён в экранированной камере.

Название организации, выполнившей специальные исследования (лицензиата), ссылка на лицензии и название объекта специальных исследований.

Перечисление выделенных помещений, в которых размещены исследуемые ВТСС.

Цель исследований.

Вид проводимого контроля (аттестационный или текущий). Обязательное указание этого параметра связано с тем, что при аттестационных специальных исследованиях необходимо проводить исследования всех технических средств (ТС), а при текущих — допустим выборочный контроль, с соответствующим обоснованием выбора.

Место проведения специальных исследований. Многие (но не все!) технические средства могут быть исследованы не только на своем «рабочем месте», но и на разного рода испытательных стендах, имитирующих рабочие условия. Некоторые исследования вообще могут быть эффективно выполнены только в экранированной камере или на специальном стенде. Именно поэтому важно указывать что, где и в каких условиях исследовалось.

Перечень исследованных технических средств. Перечень (таблица) должен быть абсолютно полным и соответствовать аналогичному перечню в паспорте защищаемого помещения. Все технические средства указываются с их заводскими или, при отсутствии последних, с инвентарными номерами. Еще раз необходимо подчеркнуть, что в этот перечень включаются все технические средства независимо от того, образуют ли они каналы утечки или нет. В этой же таблице указывается наличие тех или иных устройств защиты (при их наличии).

Перечень измерительной аппаратуры. Как и в любом протоколе — полный перечень средств измерения с указанием Свидетельств о поверках. Для импортных средств — указание сертификатов о включении в Госреестр. При необходимости — ссылка на сертификаты ФСТЭК России.

Анализ построения систем вспомогательных технических средств на объекте эксплуатации. Важнейший раздел для данного вида работ. Без правильного анализа всех систем и однозначных выводов из него невозможно правильно организовать и выполнить специальные исследования.

Обязательному анализу подлежат следующие системы и подсистемы, которые могут встречаться на объектах специальных исследований:

- электропитание;
- телефония (местная и городская, директорская, диспетчерская, технологическая и т. п.);
- сигнализация (пожарная и охранная, тревожная);
- радиотрансляция;
- система оповещения;
- местная громкоговорящая связь;
- часофикация;
- ЛВС (локальная вычислительная сеть);
- видеонаблюдение;
- прием телевизионных программ (центральное и местное вещание, технологическое ТВ и др.);
- музыкальные центры, тюнеры и другие радиоприемные и усилительные устройства;

- средства записи и воспроизведения информации (магнитофоны, проигрыватели, плееры и т. п.);
- системы автоматики устройств вентиляции и кондиционирования воздуха;
- СКД (системы контроля доступа);
- электрозамки;
- устройства бытовой техники (холодильники, микроволновые печи, чайники и др.);
- блоки питания различного назначения (зарядные устройства, АБП и др.).

Целью данного анализа является доказательное определение для *каждого* из технических средств (группы ТС), размещенных в выделенном помещении, выходят ли отходящие от него линии (электропитания, слаботочные, любые) за пределы установленной контролируемой зоны. Причем опасными признаются только гальванически непрерывные линии. Существует еще и канал утечки за счет параллельного пробега проводов, линий, кабелей и т. д. Однако в связи с достаточной сложностью проблемы ограничимся только его упоминанием.

В этом смысле выход за пределы контролируемой зоны линии от «сухих контактов» реле часто не рассматривается как опасный, хотя и далеко не всегда. Выход линии через трансформатор — более сложный случай и должен оцениваться отдельно. Во многих случаях трансформатор не является серьезным препятствием на пути распространения опасного сигнала. Выход линии через преобразование «ЦАП-АЦП» (в цифровых АТС) или через частотный модулятор (модем), как правило, рассматривается как безопасный для слабых опасных сигналов типа прямого акустоэлектрического преобразования. Однако бывают исключения, требующие инструментального контроля.

Изложить в данном курсе все возможные ситуации не представляется возможным. Однако еще раз напомним, что описание конкретной подсистемы (при необходимости с приложением плана размещения ее элементов, функциональных и принципиальных схем) должен *доказательно и однозначно* отвечать на вопрос: имеется ли выход линий от данного технического средства за пределы контролируемой зоны или нет.

Хочется обратить внимание на то, что этот анализ достаточно трудоемок, требует привлечения многочисленных специалистов различных обслуживающих структур организации. Выполнять его во время проведения специальных исследований можно, но это время и, следовательно, деньги. Гораздо целесообразнее заказчику заранее, без особой спешки, на стадии подготовки собрать всю необходимую

информацию, подготовить документы и не тратить время лицензиата на то, что можно и нужно выполнить самим.

В выводах данного раздела протокола коротко резюмируется, какие именно технические средства имеют линии, выходящие за пределы контролируемой зоны и что это за линии. Соответственно, перечисляются линии и ТС, для которых должны быть выполнены контрольные измерения.

Основные положения методики исследований. В данном разделе перечисляются либо ссылки на использованные методики, либо дается их очень краткое изложение. Особо излагаются (рекомендуется с обоснованием) принятые изменения или отступления от существующих (утвержденных) методик.

Следует отметить, что в настоящее время формально отсутствуют методические материалы в этой области, оформленные законодательным образом. Существует ведомственный сборник методик, разработанный НИИА (Министерство промышленности средств связи СССР) еще в 1978 г. Тогда он был согласован с Гостехкомиссией СССР. В настоящее время это единственный сборник методик в области акустоэлектрических преобразований. Хотя данный сборник не учитывает целые классы новых технических средств, но во многих вопросах еще актуальный. К глубокому сожалению, пока других нет. Толкование и применение некоторых его положений уже давно вызывает споры. Например, в области измерений прямого акустоэлектрического преобразования эта методика предписывает применение, в том числе, широкополосного метода измерений. Такой метод мог применяться к техническим средствам, микрофонный эффект которых в сотни и тысячи раз превышает нормы. Такие технические средства встречаются крайне редко. Однако иногда контролирующие органы, не на чем реальном не основываясь, настойчиво требуют его применения ко всем техническим средствам.

Основная, узкополосная методика исследования прямого акустоэлектрического преобразования направлена на определение не величины опасного сигнала в отходящей линии (эта величина в методике является промежуточной), а на определение коэффициента акустоэлектрического преобразования (своеобразной чувствительности технических средств к акустическому воздействию). В то же время в «Нормах...» заданы именно предельно допустимые величины напряжения опасного сигнала. Однако «Нормы...» переутверждены уже в недавнее время и являются более весомым документом, что и следует учитывать в работе.

Можно привести еще ряд подобных же примеров. Именно поэтому важно грамотное и доказательное составление данного раздела протокола.

Результаты специальных исследований технических средств. В этом разделе приводятся результаты измерений и расчетов по каждому из исследованных технических средств.

В начале раздела, в нескольких общих пунктах, рекомендуется перечислить те технические средства, специальные исследования которых не проводятся с обязательным указанием причин. Обычно это:

- ТС (для прямого АЭП), не имеющие линий, выходящих за пределы КЗ;
- ТС, не образующие канала утечки по своим конструктивным особенностям (и для прямого, и для модуляционного АЭП);
- ТС, отключаемые на время проведения закрытых мероприятий по каким-либо другим требованиям.

При выборочном контроле перечислить с указанием причин, какие именно технические средства не измерялись, а также указать критерии отбора проверяемых технических средств.

Рекомендуется данный раздел подразделять на измерения прямого акустоэлектрического преобразования и модуляционного акустоэлектрического преобразования. Это поможет более легко и удобно понимать рассматриваемые вопросы. Примеры записи результатов, таблиц, выводов и т. д. приведены в Приложении.

Все оставшиеся технические средства, перечисленные в таблице, должны быть измерены, а результаты приведены в данном разделе.

Отдельно рассматриваются случаи, когда применены те или иные устройства защиты. При наличии таковых должны быть проведены исследования, подтверждающие их работоспособность и эффективность. Вполне рядовой вариант, когда опасный сигнал на линии некого устройства ВТСС во много раз превышает норму, но установленное в линии устройство защиты понижает его в такой степени, что норма выполняется. Это должно быть показано в цифрах. К сожалению, не так редки случаи, когда устройство защиты либо неправильно эксплуатируется, либо вышло из строя.

Заключение. В данном разделе в краткой форме приводятся сводные данные по всем техническим средствам (защищено, не защищено, защищено при таких-то условиях). В состав раздела могут включаться рекомендации по защите тех или иных технических средств.

Средства измерения. В соответствии с нормативными документами и постановкой задачи специальные исследования акустоэлектрических преобразований сводятся к измерениям слабых (как правило) сигналов речевого диапазона частот (300 Гц. . . 3,4 кГц, в настоящее время этот диапазон расширен) или ВЧ сигналов (до $\approx$2000 МГц) и определению коэффициента модуляции (для АМ) или индекса моду-

ляции (для ЧМ) этих ВЧ сигналов теми же сигналами речевого диапазона.

Отсюда и требования к средствам измерения. Это селективные измерительные приборы речевого диапазона частот (селективные вольтметры, анализаторы спектра, микро- и нановольтметры) и измерительные приемники или анализаторы спектра в диапазоне частот минимум до 2000 МГц.

Так как нормированные коэффициенты и индексы модуляции имеют достаточно малые величины, особенно важно учитывать, чтобы приборы ВЧ диапазона имели при высокой чувствительности как можно более низкие собственные шумы. Именно при специальных исследованиях акустоэлектрических преобразований чаще всего приходится производить и измерения, и расчеты «по шумам». Как отмечалось выше, в этом случае оценка защищенности напрямую зависит от технических характеристик средств измерения.

Исходя из вышеизложенного, для исследований в области ВЧ диапазона принципиально наиболее пригодными являются измерительные приемники, всегда имеющие более низкие собственные шумы, чем анализаторы спектра. Из аппаратуры 1970-х годов это, практически без исключений, измерительные приемники RFT (бывшая ГДР) моделей FSM-6, FSM-11 и FSM-8. Перекрывая диапазон от 0,1 (0,01) до 1000 МГц (два приемника), они и до сих пор остаются весьма надежными, чувствительными, с хорошими детекторами и малошумящими средствами измерений. К тому же их стоимость относительно невелика.

Из современных приборов наиболее пригодными являются измерительные приемники, например, серий ESIB или ESPI фирмы R&S. Параметры их очень высоки, например собственные шумы приемника ESPI3 с опцией перестраиваемого предусилителя составляют не более −157 дБм (для сравнения: у анализатора спектра 4407 фирмы Agilent Technology — не более −130 дБм). Но и стоимость таких приемников весьма высока.

К вышесказанному необходимо добавить различные антенны — дипольные (электрические) и рамочные (магнитные), предусилители, различные симметрирующие устройства (часто приходится выполнять замеры в симметричных линиях), токовые трансформаторы, пробники. Моделей таких устройств множество, хотя заметная часть их имеется только импортного производства и тоже недешева. Однако вполне приличные антенны выпускаются и у нас в стране, как и предусилители и токовые трансформаторы.

В области низких звуковых частот по-прежнему вне конкуренции очень старенькие, но еще работающие селективные нановольтметры производства предприятия Unipan (бывшая ПНР). Это модели Unipan

233, 237 и 232b. Если моделям 233 и 237 были аналоги (иногда с более высокими параметрами, например FAT-2, FAT-3, R&S ФРГ), то фазочуствительный микровольтметр 232b и по сей день остается уникальным прибором. Его применение позволяет «вытянуть» сверхслабые сигналы «из-под шумов», по крайней мере на уровне −20 дБ эффективнее, чем любым другим прибором. Именно потому он и остается ещё и на сегодняшний день рабочим средством измерения в этой области. Кроме того, эти вольтметры комплектуются набором предусилителей с симметричными и несимметричными входами с уникально (и по сей день!) низкими собственными шумами.

Для низкочастотной области также существуют современные анализаторы спектра. Однако большинство моделей не могут быть рекомендованы из-за достаточно высоких собственных шумов и очень высокой стоимости.

Кроме основных средств измерения, необходимо много вспомогательных нестандартных приспособлений и устройств. В первую очередь это источник акустического тест-сигнала. Таких источников необходимо минимум два для решения разных задач (не всегда удобно объединять их в одно устройство, хотя это и возможно).

Первый источник должен создавать плавно перестраиваемый по частоте акустический сигнал в диапазоне не менее 100 Гц... 10 кГц. Обычно это легко решается комбинацией звукового генератора, усилителя и колонки. Вроде бы ничего особенного. Однако основным требованием к такому устройству является отсутствие от него побочных излучений с частотами генерируемых сигналов как по электрическому, так и, что гораздо сложнее, по магнитному полю. Даже небольшая наводка по магнитному полю на исследуемые ВТСС во многих случаях значительно превышает сигналы акустоэлектрических преобразований. Ни один типовой усилитель, тем более колонка, этим требованиям не удовлетворяет. Такой источник должен проектироваться специально и тщательно экранироваться (включая все кабели и цепи электропитания). Примером такого источника может служить усилитель-генератор тест-сигналов «Шорох-2МИ» со специальной экранированной колонкой УЭК.

Второй источник должен давать акустический сигнал в виде одной–двух хорошо слышимых человеком частот (обычно в диапазоне 400... 1500 Гц), манипулируемых по амплитуде частотой 0,1... 5 Гц (так сказать, прерывистая «пищалка»). Эти сигналы хорошо опознаются оператором «на слух» при выявлении модуляции различных генераторов в ВТСС при акустическом воздействии на них. Такие источники выполняются, как правило, автономными (и с автономным питанием) и тщательно экранированными. Серийное производство таких генераторов тест-сигнала, по нашим данным, в настоящее

время отсутствует и, в основном, многие организации, проводящие специсследования, разрабатывают их самостоятельно.

Также необходим стандартный шумомер с микрофоном, поскольку методики требуют точного замера величины действующего на ВТСС акустического сигнала. Останавливаться на этой аппаратуре не имеет смысла, так как она подробно описана выше.

Кроме этого, необходимы осциллографы (желательно двулучевые и широкополосные), генераторы стандартных сигналов на весь исследуемый диапазон (желательно с цифровой установкой частоты и амплитуды, например IFR 2325), обычные широкополосные вольтметры В3-38, В3-57, генераторы НЧ Г3-112 и множество мелочей типа коаксиальных переходов, кабелей разного рода, пробников, аттенюаторов, коаксиальных трансформаторов и т. д.

Примечание. В разделах, посвященных средствам измерения, намеренно приведены достаточно старые модели приборов общего назначения. Многие из них еще успешно эксплуатируются. Современные приборы с аналогичными и более высокими характеристиками (генераторы, вольтметры, осциллографы и т. д.) без труда могут быть приобретены в специализированных фирмах.

Это дополняется нестандартным оборудованием типа «питающего моста», имитирующего подачу питания на телефонные аппараты, различными устройствами, позволяющими имитировать нормальный рабочий режим исследуемого ВТСС, его электропитание различными напряжениями (типа испытательных стендов), фильтрами различного диапазона и назначения (помехоподавляющие — сетевые и сигнальные, режекторные, полосовые и т. п.) и, наконец, очень нелишней будет экранированная камера. Сооружение весьма недешевое, но крайне эффективное, когда нужно измерять микровольтовые сигналы в условиях помех большого города.

До последнего времени нельзя было назвать современные разработки измерительных приборов и систем, специально предназначенных для выполнения исследований в области АЭП. Теперь такие приборы и системы есть. Однако ориентироваться в предложениях на рынке не так просто. За время, прошедшее с момента выхода первого издания этой книги, в предложениях появилось достаточное количества приборов и систем, в информационных материалах о которых указано, что они способны измерять акустоэлектрические преобразования. Не будем заниматься «антирекламой» и называть фирмы-производители поимённо. Читатель вполне разберётся и сам, напомним лишь, что средством измерения считается прибор, внесённый в Госреестр.

Однако следует обратить внимание, что внесённый в Госреестр прибор должен проводить измерения точно в соответствии с формули-

ровкой, записанной в описании этого средства измерения. Результат прямого низкочастотного АЭП — переменное напряжение электрического тока. Такая физическая величина измеряется в вольтах, и прибор, её измеряющий, называется вольтметром (селективным вольтметром). Так и только так должна читаться основная формулировка в описании прибора. Если средство измерения не является вольтметром, то правомочность измерения им напряжения вызывает вопросы.

Рассматривать разработки, не имеющие метрологического сертификата, просто не имеет смысла. Равно как и попытки применять для измерения напряжения приборы, метрологически аттестованные для измерения иных физических величин (звукового давления, вибраций, и т. д.). Собственно, после селекции по вышеприведённым критериям в рассмотрении остаётся две разработки — «Гриф-АЭ1001» и система «Талис».

Рассмотрим их чуть подробнее.

Изделие «Гриф-АЭ1001» появилось несколько ранее. Оно представляет собою специализированный цифровой селективный вольтметр-анализатор спектра, хотя его разработчики и не сформулировали описание типа в соответствии с выше приведенным критерием. Прибор состоит из малошумящего усилителя звукового диапазона частот с последующей оцифровкой усиленного сигнала АЦП. Далее цифровой поток поступает в хост-машину (типовой ноутбук), где программно реализованный преобразователь Фурье (БПФ) строит спектр сигналов. Там же, программно, реализованы функции графического пользовательского интерфейса управления и расчётная задача. Тот же (или аналогичный) тракт измерения, в другом режиме, используется для измерения звукового давления тест-сигнала. Система формирования акустического тест-сигнала выполнена отдельно на базе активной экранированной колонки-генератора. Прибор управляется полностью вручную, включая канал тест-сигнала. Входное сопротивление тракта измерения 600 Ом или 1 МОм. В комплект включены электрическая и магнитная антенны для измерения напряжённости полей (в описании типа не названа функция измерения напряжённости поля). Не приводя подробных данных, укажем основные достоинства и недостатки прибора.

Прибор позволяет выполнять СИ АЭП в НЧ диапазоне, имеет сертификат средства измерения военного назначения и сертификат ФСТЭК России.

Для исследований ВЧ АЭП, т. е. паразитной модуляции, прибор не предназначен.

Хорошее разрешение по частоте (до 1 Гц), относительно небольшие габариты и достаточно низкий уровень собственных шумов по-

Рис. 5.46. Система «Талис»

зволяет считать прибор достаточно эффективной заменой «умирающим» вольтметрам Unipan.

Однако необходимо отметить, что наблюдается неустойчивая работа ПО; чувствительность прибора, его антенн и измерительного входного кабеля к воздействию акустического тест-сигнала; довольно высокий уровень паразитного излучения колонки по магнитному полю и чисто ручное управление. Это заметно снижают пользовательскую привлекательность данного изделия.

Отмечены при эксплуатации и флуктуации погрешности измерений, класс точности прибора не приводится.

Система «Талис» (рис. 5.46) в её полнофункциональном виде состоит из двух полностью автоматизированных систем, поставляемых совместно либо раздельно.

Собственно система «Талис» предназначена для поиска и выявления компонент ПЭМИН штатных автогенераторов технических средств и измерения паразитной модуляции при воздействии на исследуемое ТС тестового акустического сигнала от системы «Талис».

Система «Талис-НЧ» (рис. 5.47) предназначена для автоматизированных измерений результатов АЭП в отходящих от исследуемого ТС линиях.

Обе системы (подсистемы) имеют сертификаты средств измерения военного назначения. В описаниях типа, в соответствии с областью применения, система «Талис» определена как измеритель напряжённости полей, ВЧ токов в линиях и измеритель параметров моду-

Рис. 5.47. Система «Талис-НЧ»

ляции. Система «Талис-НЧ» описана как селективный вольтметр. Система «Талис» также имеет сертификат ФСТЭК России.

Не вдаваясь в технические подробности обоих систем, укажем, что «Талис»+ «Талис-НЧ» является автоматизированной системой, способной выполнять весь комплекс СИ АЭП в автоматическом режиме. При этом такой комплекс может измерять параметры модуляции до 10^{-5} (уникальный показатель, не имеющий аналогов в мире), чувствительность всех элементов системы «Талис-НЧ» к акустическому воздействию гарантированно ниже измеряемых сигналов, побочные поля рассеяния акустического излучателя крайне малы, входное сопротивление измерителя не ниже 10 МОм. Погрешности при измерениях напряжённости полей не превышают 2 дБ, при определении уровня модуляции — не более 10 %, при измерении НЧ сигналов от 50 нВ до 8 В — не более 1 дБ.

Система «Талис-НЧ» способна выполнять измерения в линиях электропитания без отключения промышленной электросети. Подавление частот 50, 100 и 150 Гц превышает 120 дБ. Все измерения могут выполняться по заранее сформированному заданию без участия оператора. Результаты измерений и расчётов выдаются в виде технического протокола в формате MS Word.

Незначительные дополнения системы «Талис» превращают её в универсальный измерительный комплекс, способный выполнять весь объём СИ для типовых ТКУИ (АВАК, АЭП, и ПЭМИН). Продолжают-

ся работы по модернизации системы, уменьшению массогабаритных и стоимостных показателей.

Разумеется, и система «Талис» не лишена недостатков. Она имеет высокую стоимость, относительно большие габариты, интерфейс управления достаточно сложен. Наверное, в процессе эксплуатации у пользователей появятся ещё замечания и пожелания.

5.2.6. Особенности СИ в области акустоэлектрических преобразований

В таком кратком курсе, как этот, невозможно рассказать обо всех возможных «тонкостях» измерений в этом виде СИ. Однако попытаемся изложить самое основное. Вначале придется коснуться физики происходящих процессов, поскольку без ее правильного понимания невозможна организация измерительных работ и выявление возможных ошибок и помех.

Итак, что же является физической основой того, что принято называть акустоэлектрическим преобразованием? В качестве преобразователей механической энергии акустического сигнала в электрические могут выступать элементы технических средств, обладающие различной природой и достаточно широким спектром физических свойств.

В первую очередь, это эффект, открытый в 1831 г. Фарадеем. Суть его в том, что при движении проводника поперек силовых линий магнитного поля на его концах наводится ЭДС (при замкнутом проводнике течет ток). Магнитное поле существует всегда (существует магнитное поле Земли, необходимо помнить о том, что любая деталь из сплавов железа, некоторых других металлов и их сплавов всегда намагничена). Следовательно, перемещение любого проводника (вибрация, дрожание), особенно многовитковой обмотки, неизбежно вызывает появление напряжения или тока, соответствующих акустическому (вибрационному) воздействию. Поэтому все моточные изделия (трансформаторы, реле, катушки индуктивности, дроссели и т. д. в составе ВТСС) всегда являются источниками акустоэлектрических преобразований. Кроме того, возникающая под воздействием акустических сигналов вибрация всякого рода сердечников перечисленных компонентов (это более характерно для материалов с высокой магнитной проницаемостью μ) вызывает (за счет волн сжатия в материале) изменение их магнитной проницаемости (обратный магнитострикционный эффект, или эффект Веллари), что также вызывает появление сигнала в обмотке.

Вторая причина, — различные емкостные эффекты. Если в конденсаторе, образованном некими проводящими элементами, одна обкладка движется относительно другой, изменяется емкость этого кон-

денсатора, следовательно, меняется напряжение на обкладках. Механические напряжения в диэлектриках приводят к изменению их диэлектрической проницаемости и, как следствие, к изменению ёмкости.

Третий, весьма часто встречающийся эффект — пьезоэффект. Большое число керамических конденсаторов выполняется из материалов типа ЦТС (цирконий – титанат свинца) или аналогичных. Такие материалы всегда обладают пьезострикционным эффектом, т. е. при приложении к ним механического усилия (изгиб, сдвиг, сжатие и т. д.) на обкладках конденсатора генерируются электрические потенциалы, пропорциональные приложенному усилию. Короче говоря, нормальный пьезоэлектрический микрофон.

Есть еще ряд более «тонких» эффектов, но и этого достаточно, чтобы понять основной «закон» — *«Микрофонит все!»* И только измерениями можно доказать, что в каждом данном конкретном случае и при строго определенных режимах работы технических средств сигнал акустоэлектрического преобразования меньше нормы. Других способов не существует.

Все изложенное выше касается прямого низкочастотного акустоэлектрического преобразования. Однако необходимо помнить, что в составе многих технических средств всегда, штатно, работают один или несколько разного рода ВЧ автогенераторов, как синусоидальных, так и релаксационных. Воздействие на их элементы (конденсаторы, дроссели, системы заряженных проводников и т. д., о чем говорилось выше) механических колебаний (акустических сигналов) в общем случае *всегда* (вопрос только в какой степени) приводит к изменению амплитуды и/или частоты/фазы этих колебаний, т. е. к модуляции. ВЧ колебания этих генераторов в той или иной степени излучаются в окружающее пространство и/или распространяются по отходящим от технических средств линиям. Так образуются модуляционные высокочастотные каналы акустоэлектрических преобразований, которые опасны не сами по себе, а именно тем речевым сигналом, который модулирует ВЧ колебания автогенераторов. Для этих каналов приходится учитывать и величину (амплитуду) несущей и коэффициент (индекс) модуляции.

Познакомившись вобщем с причинами появления сигналов АЭП, рассмотрим основные схемы измерений.

Так как задачей для прямого акустоэлектрического преобразования является определение значений сигналов АЭП речевого диапазона частот в отходящей от ВТСС линии, выходящей за пределы КЗ, то типовая схема измерения приведена на рис. 5.48.

Исследуемое техническое средство может быть подключено к реальной отходящей линии, к некому имитатору или не подключаться ни к какой линии (режим «холостого хода»). Рассмотреть все возможные

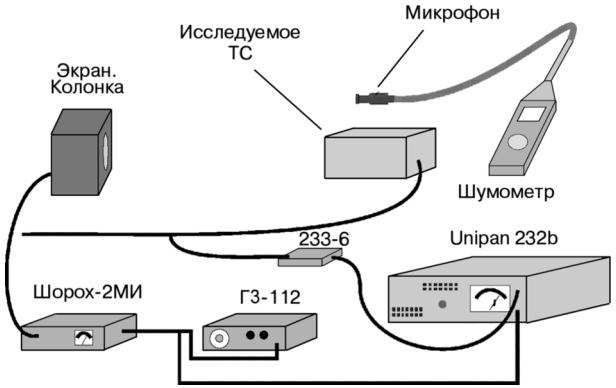


Рис. 5.48. Типовая схема измерения прямого АЭП при помощи стандартных измерительных приборов

варианты и их особенности в рамках этого курса не представляется возможным, ограничимся только перечислением этих вариантов.

К отходящей линии (или к выходному разъему ВТСС) подключается измерительный прибор. Причем это подключение может быть гальваническим (как показано на рис. 5.48) или бесконтактным (с помощью токового трансформатора).

Во всех случаях необходимо проводить измерения для всех возможных вариантов подключения: симметрично, несимметрично, два провода — «земля», так называемая цепь Пикара, по «разбитым» парам, если количество проводов более двух, по отношению к посторонней земле, два (или несколько) проводов вместе с использованием трансформатора тока или любым другим способом. Потенциальный противник всегда будет искать способ подключения с наилучшим отношением сигнал/помеха. Выбор из этого множества вариантов ложится на заказчика или, если заказчик не определяет область исследований, на исследователя.

Гальваническое подключение осуществляется, как правило, через стандартный предусилитель вольтметра (например, типа 233-5, 233-6, 233-7 нановольтметров Unipan). Установка токового трансформатора может производиться на один провод линии или на несколько одновременно, выбирая наилучшую комбинацию с точки зрения перехвата. Кроме того, применяя токовый трансформатор, необходимо учитывать, что он измеряет ток в линии, а нормируется напряжение в ней. Следовательно, необходим пересчет результатов измерений через эквивалентное сопротивление линии или источника сигнала АЭП.

Исследования любого технического средства необходимо проводить во всех возможных режимах его работы, если не оговаривается перечень режимов, при которых техническое средство будет работать

при эксплуатации. Так, например, исследования многоскоростного бытового вентилятора необходимо проводить при включении его на разных скоростях с учетом допустимых отклонений напряжения питания при проведении измерений для каждой скорости. За конечный результат должно приниматься наибольшее значение опасного сигнала из всех измеренных при различных режимах. В установках прямой директорской (диспетчерской) связи, в которых существуют телефонный (на микротелефонную трубку) и громкоговорящий (на микрофон и динамик) режимы, исследования необходимо проводить как в том, так и в другом режиме, если в задании на проведение измерений не указан только какой-либо один рабочий режим. И таких примеров может быть множество.

Во всех случаях в протоколе исследований необходимо указывать все возможные режимы работы ТС с обоснованным указанием, по каким причинам тот или иной режим работы не проверялся.

Схема измерения сигналов АЭП от ТС, приведенная на рис. 5.48, достаточно стандартна для выполнения измерений и особых пояснений, на наш взгляд, не требует. Если же для исследования применяется автоматизированная система «Талис-НЧ», то схема измерений выглядит так, как на рис. 5.49.

В приведённых схемах опущены очень важные на практике вопросы заземления приборов, их электропитания, взаимного размещения. Необходимо отметить, что уровень помех в тракте измерения от этих факторов может меняться в десятки и сотни раз. Неоптимальное построение измерительного комплекса может быть причиной очень далеких от реальности результатов.

Борьба с помехами в измерительных трактах хорошо освещается в теории радиоизмерений и измерений в технике связи; все общие принципы этой теории справедливы и для данной методики, а дать рекомендации по многочисленным нюансам каждой конкретной измерительной схемы просто не представляется возможным. Данную задачу решает каждый оператор самостоятельно, опираясь на свой опыт, знание предмета измерений и в какой-то степени — интуицию.

Учитывая степень малости измеряемых сигналов акустоэлектрических преобразований, определяющее внимание следует уделить снижению наводок тест-сигнала на измеряемое техническое средство и измерительный приемник.

Как правило, экранированную колонку размещают на расстоянии 1 м от исследуемого технического средства. Это расстояние не очень критично и выбирается, в первую очередь, исходя из требуемого уровня звукового давления в месте размещения технического средства и отсутствия наводок от колонки на исследуемое ВТСС.

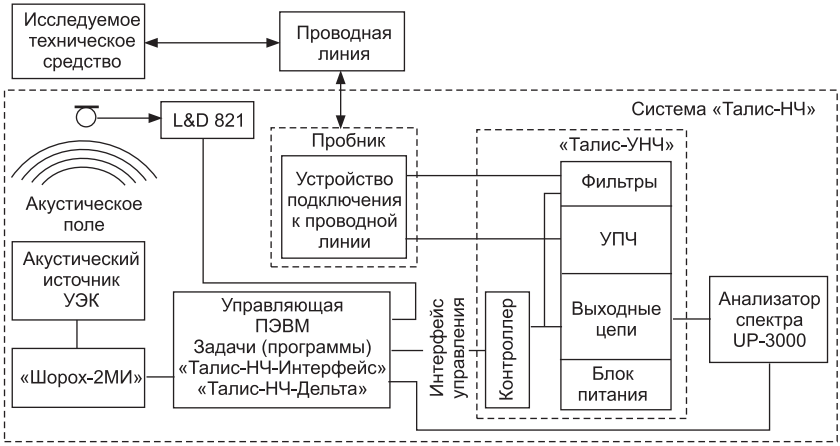


Рис. 5.49. Функциональная схема измерения прямого АЭП при помощи системы «Талис-НЧ»

Понятно, что даже хорошо экранированная колонка создает некоторые электрическое и магнитное поля, наводки от которых не должны вносить погрешности в измерения. Простейший способ определения того, что мы наблюдаем — наводку тест-сигнала от акустического излучателя, измерительного тракта генератор-усилитель мощности и соединительных кабелей или непосредственно сигнал АЭП, состоит в прикрывании лицевой панели акустического излучателя звукопоглощающей шторкой с целью изменения (снижения) уровня воздействующего на ТС акустического сигнала, контролируемого с помощью шумомера. При этом наводка за счет воздействия электромагнитного поля генераторного оборудования на техническое средство, если она существует, останется неизменной, т. е. показания измерительного прибора, подключенного к техническому средству, не изменятся или, в крайнем случае, изменятся непропорционально снижению уровня акустического сигнала. В первом случае измеряемая величина тест-сигнала — «чистая» наводка, во втором — смесь сопоставимых по уровням сигналов наводки и акустоэлектрических преобразований.

Другим, достаточно эффективным способом определения достоверности измерения именно сигнала акустоэлектрического преобразования при той же измерительной схеме является изменение расстояния между генераторным оборудованием, включая акустический излучатель, и исследуемым техническим средством. При линейном изменении сигнала акустоэлектрического преобразования от расстояния измеряемый сигнал является следствием акустического воздействия на техническое средство, а при изменении измеряемого сигнала по закону $1/R^2 - 1/R^3$ — наводка за счет электрического или маг-

нитного полей генераторного оборудования. Этим способом удобно пользоваться для определения того, какая из составляющих электромагнитного поля преобладает в сигнале наводки. При изменении сигнала по закону близкому к $1/R^3$ наводка определяется преимущественно магнитным полем, при изменении по закону $1/R^2$ — электрическим полем. Понимание природы образования сигнала наводки определяет и меры борьбы с ней. При электрической наводке, как правило, бывает достаточно организовать правильную схему заземления измерительного комплекса в целом. При магнитной наводке значительное снижение можно получить только симметрированием, применением экранированных симметричных кабелей со скрученными парами и разносом элементов измерительного (генераторного) тракта и технических средств.

5.2.7. Общий порядок проведения измерения

Собрать схему измерительного стенда, включить, прогреть и откалибровать все средства измерения. Далее оператор плавно изменяет частоту звукового генератора в требуемом диапазоне частот, поддерживая звуковое давление на исследуемое ВТСС в диапазоне 80...100 дБ. Обычно огибающая сигналов АЭП имеет резко изрезанный характер с пиками и провалами. Рекомендуется фиксировать все пики сигнала. Если их много, то наибольшие. При использовании нановольтметра 232b не забывать тщательно подстраивать фазу опорного сигнала на каждой подозрительной частоте.

Особо следует заметить, что задавать заранее какой-либо шаг частот методически абсолютно неверно. Пики и выбросы сигнала АЭП могут возникнуть на любой частоте, а механические резонансные явления, которые обычно ответственны за такие выбросы, бывают весьма узкополосными. Испытание плавно меняющимся тоном — принципиальное методическое требование. Если используется генератор низкой частоты с дискретной перестройкой, то нужно перестраиваться с шагом не более 10 Гц. Да и то это эмпирическая рекомендация, основанная на статистических данных.

Действующие методики имеют достаточно обобщенный характер и не могут в силу этого отразить всего многообразия их применения при проведении специальных исследований. Так, например, при исследовании сигналов АЭП в сети электропитания технических средств промышленной частоты 220 В (50 Гц), как указывалось выше, необходимо проводить измерения и при включенной, и при отключенной сети электропитания, причем независимо от того, где располагается высоковольтная трансформаторная подстанция, в пределах контролируемой зоны объекта или за ее пределами, — непреднамеренное (а хуже того — преднамеренное) отключение сети электропитания возможно

и в том, и в другом случае. В первом случае оценку следует давать по нормам сети питания и только по несимметричной составляющей, а во втором — по нормам для линий связи при всех возможных вариантах подключения измерительного приемника к сети питания или сетевому шнуру ТС. В то же время при гарантированном питании объекта категории не ниже первой или особой группы первой категории (о чем в обязательном порядке у заказчика должен быть утвержденный «Акт...») проводить исследования в сети питания в режиме ее отключения нет необходимости. При бесперебойном питании, при кажущейся более высокой степени надежности электропитания, объем измерений в значительной степени увеличивается по сравнению с питанием гарантированным. Это объясняется несколькими причинами:

- в большинстве агрегатов бесперебойного питания (АБП) имеется функция «обхода», при включении которого исследуемая сеть становится обычной негарантированной с соответствующими к ней подходами;
- сеть электропитания, организованная с использованием АБП, в общем случае не может относиться с точки зрения защиты информации к сети питания промышленной частоты (так называемая «чистая» сеть с точки зрения наличия в ней помех), в связи с чем на данную сеть распространять нормы для сети питания некорректно;
- как следствие изложенного в предыдущем пункте, для оценки защищенности сети с АБП необходимо проводить измерение обратного затухания АБП, т. е. использовать агрегат только как буферное устройство, вносящее некоторое и всегда конечное затухание сигналам АЭП; сразу стоит отметить, что задача измерения обратного затухания АБП под нагрузкой не самая простая;
- всегда следует помнить, что время работы АБП конечно и ни каким образом не связано со временем возможного отключения сети.

Всех такого рода (или любого другого) частных случаев методика проведения специальных исследований, естественно, содержать не может (вспомним о проведении подробного анализа, о котором говорилось ранее). Образно говоря, именно поэтому специальные исследования названы не измерениями, а именно исследованиями, и каждый, работающий в этой области знаний, должен быть именно исследователем.

Следует акцентировать внимание еще на одну достаточно распространенную ошибку при проведении специальных исследований в части акустоэлектрических преобразований технических средств — подобные преобразования могут возникнуть при наличии разнообразных средств защиты от утечки за счёт АЭП.

При применении указанных средств на объектах заказчика даже среди специалистов в области специальных исследований бытует достаточно распространенное мнение о том, что применение сертифицированных средств защиты или типовых схем защиты, предусмотренных регламентирующими документами, не требует проверки их эффективности.

Приведем простой пример. Многочисленными исследованиями доказано, что уже применение правильно спроектированного 4-каскадного транзисторного усилителя в режиме «А» без обратной связи (ООС) с трансформаторными входом и выходом при хорошем экранировании как самого усилителя, так и отдельно трансформаторов, обеспечивает обратное затухание примерно 120 дБ. Введение в таком же усилителе 100 % отрицательной обратной связи для улучшения характеристик самого усилителя снижает обратное затухание практически до 0, а применение местных ООС в различных комбинациях в каждом конкретном случае будет изменять обратное затухание на определенную величину, характеризующую только данную комбинацию ООС. В то же время регламентирующим документом допускается использование в ВП 3-й категории абонентских громкоговорителей, обладающих чрезвычайно высокими уровнями сигналов АЭП (достигающих 10 и более мВ) с применением буферного усилителя, размещаемого в пределах КЗ, без каких-либо ограничений на его параметры и проверки его параметров. В общем случае — это нонсенс.

Еще один пример. Паспортными данными на изделие МП-2, имеющего сертификат Гостехкомиссии России, определено напряжение шумового сигнала на выходе устройства без нагрузки в пределах от 1 до 2 мВ. Устройство предназначено для защиты трехпрограммных громкоговорителей по цепи радиотрансляции, полоса пропускания в НЧ диапазоне которых в соответствии с ГОСТом должна быть не менее 10 кГц. Логично предположить, что измерение шумового сигнала следует проводить также в полосе примерно 10 кГц или еще проще широкополосным среднеквадратичным вольтметром. Однако при всей логичности такого подхода именно здесь кроется достаточно часто повторяемая ошибка, заключающаяся в следующем:

- при измерении с помощью только вольтметра вполне вероятно допустить ошибку, приняв измеренные, например, высшие гармоники сети питания громкоговорителя и продукты преобразования выпрямителя, проникающие в абонентскую линию, за шумовой сигнал при неисправном генераторе шума;
- применение осциллографа совместно с вольтметром существенно увеличивает шансы на получение относительно достоверных измерений, но полностью не исключает допущения значительной

ошибки, так как определить соответствие спектра шумового сигнала заданному практически не представляется возможным.

Единственно правильным решением оператора при проверке эффективности данного устройства (только в части работоспособности генератора шума, так как устройство МП-2 обеспечивает и ряд других функций) будет исследование спектральной характеристики с помощью узкополосного (селективного) вольтметра или анализатора спектра с одновременным измерением широкополосного шумового сигнала.

И последний пример. В первой главе уже приводился пример с акустическими колонками в ЗП. Вполне допустим вариант, при котором граница контролируемой зоны проходит на небольших (до единиц метров) расстояниях от ограждающих конструкций выделенного помещения. Учитывая, что музыкальный центр, как правило, размещается вдоль стен защищаемого помещения (и не обязательно вдоль внутренних) создаваемые электромагнитные поля от громкоговорителей при акустическом воздействии на них могут быть перехвачены и за границей контролируемой зоны.

Возникает резонный вопрос, что делать в этой ситуации? Закорачивание опасно, обрыв тоже опасен. Ответ может быть только один — измерять. По измеренным значениям рассчитать размер зоны и сравнить полученный результат с расстоянием до границы контролируемой зоны. При R_2, меньшем, чем расстояние до границы контролируемой зоны, утечка информации невозможна.

Конечно, возможен и противоположный вариант. В этом случае необходимо принимать организационные меры: переместить музыкальный центр или акустические агрегаты на безопасное расстояние в пределах выделенного помещения или вынести его из выделенного помещения. В крайнем случае можно использовать и пространственное электромагнитное зашумление акустических агрегатов.

Приведенные примеры, конечно, не отражают всего многообразия ситуаций, с которыми приходится сталкиваться на объектах при проведении специальных исследований.

Одним из наиболее опасных, с точки зрения утечки информации, является канал утечки за счет модуляции колебаний встроенных в технические средства автогенераторов. Хрестоматийный пример образования такого паразитного амплитудного детектора — наводка НЧ сигнала АЭП от встроенного громкоговорителя (или выходного трансформатора УНЧ) на входную цепь тракта ПЧ супергетеродинного приемника, построенного с использованием LC-контуров, или на входные LC-цепи усилителя ВЧ сигнала трехпрограммного громкоговорителя. Чем не классический модулятор.

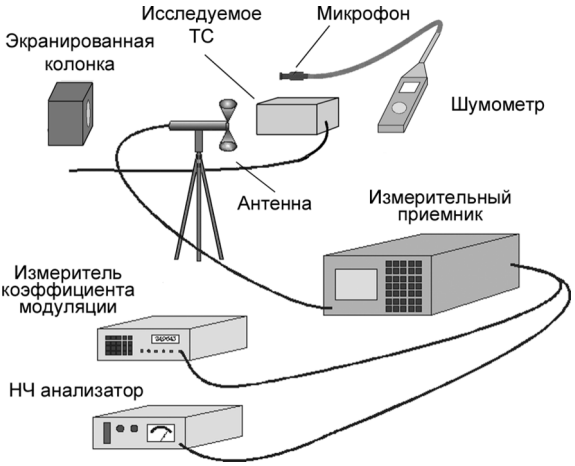


Рис. 5.50. Схема измерения модуляционного АЭП

На самом деле различного рода схем паразитных модуляторов в исследуемых технических средствах может быть великое множество. Не всегда это может приводить к образованию канала утечки, но и исключать такую возможность нельзя.

Для измерений в высокочастотной области, т. е. модуляционного акустоэлектрического преобразования схема измерений приведена на рис. 5.50.

Как видно из схемы, основой измерительного комплекса является измерительный приемник (анализатор спектра). К нему подключается либо антенна (если ведутся измерения ПЭМИ), либо тот или иной пробник или токоизмеритель (если ведутся измерения в отходящей линии), а чаще всего последовательно и то, и другое. К выходу ПЧ приемника могут подключаться либо измеритель модуляции (для непосредственного измерения), либо низкочастотные измерительные приборы (НЧ анализаторы спектра) при измерении методом боковых частот. Для выявления модуляции «на слух» на НЧ выход приемника могут включаться головные телефоны.

Если применяется автоматизированная система, такая как «Талис», то схема измерений упрощается (рис. 5.51), так как измерительный комплекс специально разработан под выполнение данной задачи.

При подготовке к проведению измерений необходимо ознакомиться с документацией на проверяемое техническое средство с целью определения принципов построения и всех возможных режимов работы изделия. Приступая к измерению, оператор должен ясно представлять себе, что, где и в каких режимах должно проверяться. Зачастую этот анализ не может быть проведен в полном объеме из-за отсут-

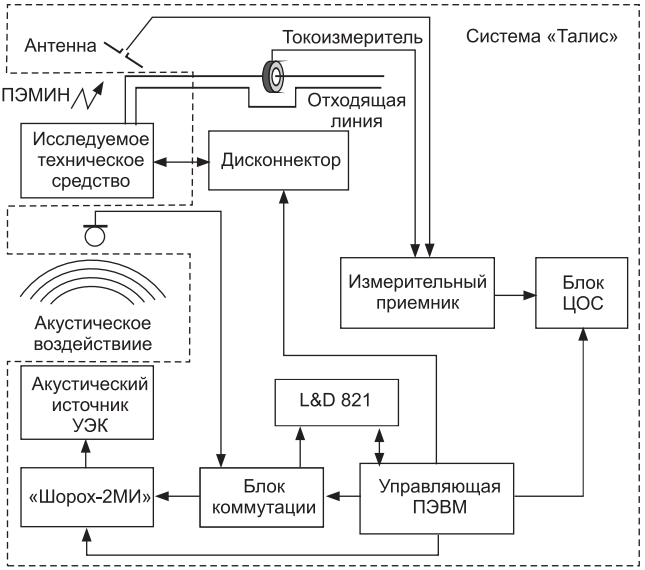


Рис. 5.51. Схема измерения модуляционного АЭП с применением системы «Талис»

ствия технической документации или неполной ясности о работе тех или иных узлов. Это, как правило, в значительной степени увеличивает время непосредственно измерений. Сразу отметим, проведение измерений без предварительного анализа, «в темную» — самый неэффективный способ, требующий неоправданно больших трудозатрат и, как правило, приводящий к серьезным ошибкам.

Первой задачей оператора является проверка всех выявленных в процессе предварительного анализа частот, обусловленных работой встроенных автогенераторов в составе технических средств, а также их гармоник. Теоретически часть этих частот при реальных измерениях может быть и не обнаружена за счет:

- существующих в эфире и отходящих от ТС линиях помех (при этом меры по борьбе с помехами должны быть приняты максимальные); здесь кстати вспомнить об экранированной камере;
- малой действующей высоты «случайных антенн», способных излучать сигналы тех или иных колебаний автогенераторов внутри самого ТС;
- преднамеренного или непреднамеренного (за счет размещения других блоков и модулей) экранирования как самих автогенераторов, так и отходящих от них физических цепей;
- наличия буферных каскадов на пути распространения сигналов автогенераторов и ряда других причин.

Эмпирических методов такого выявления довольно много, и в

настоящем курсе невозможно подробно рассказать о них всех. Каждый оператор должен решать эту задачу самостоятельно, применительно к реальным условиям проведения измерений.

Обнаружением всех частот, на которых работают встроенные автогенераторы, выявленных в процессе анализа, задача не ограничивается. Всегда существует вероятность того, что проведенный анализ не является полным. К примеру, в современных сверхбольших интегральных микросхемах, как аналоговых, так и цифровых, имеется достаточно большое количество технологических генераторов, колебания которых теоретически также вполне могут модулироваться сигналами АЭП. В супергетеродинных приемниках при преобразовании входного радиосигнала неизбежно появление так называемых зеркальных частот, что также должно учитываться при измерениях, несмотря на то что такого автогенератора в приемнике нет. И хотя разработчики современных приемников стремятся максимально уменьшить уровень сигналов на этих частотах, вероятность модуляции зеркальных частот сигналами АЭП все-таки остается. Вспомним и о возможных различного рода паразитных модуляторах, о которых было сказано выше.

В связи с этим, кроме частот, определенных в результате проведенного анализа, необходимо обязательно проводить дополнительный поиск сигналов во всем диапазоне частот от 10 кГц до 2000 МГц. Все выявленные при поиске частоты также должны проверяться на принадлежность исследуемому техническому средству и, далее, на паразитную модуляцию. В некоторых случаях обнаружение несущих частот автогенераторов и «продуктов» преобразований в ручном режиме удобно проводить, использовав в качестве источника акустического сигнала датчик тест-сигнала, создающий на выходе акустический сигнал с 1–3 частотами в речевом диапазоне, промодулированных (манипулированных) частотой 0,5...2 Гц (упомянутая выше «пищалка»). Еще лучше такой сигнал подать на вход технического средства (если есть такая возможность). Такого рода сигналы очень хорошо выявляются на слух. Естественно, такого рода предварительный анализ нельзя считать окончательным, но некоторое снижение трудозатрат всё же достигается.

На всех выявленных частотах необходимо измерить коэффициент и/или индекс модуляции акустическим сигналом. Способ определения вида модуляции (амплитудная или частотная) подробно изложен в упомянутой выше методике и приводить его здесь нет необходимости.

При проведении измерений следует иметь в виду следующее:

- при малых индексах угловой (частотной, фазовой) модуляции спектр сигнала полностью совпадает со спектром сигнала при амплитудной модуляции;

- при частотной модуляции индекс модуляции увеличивается прямо пропорционально номеру гармоники сигнала, и это еще раз подтверждает необходимость проведения исследований на максимально возможном измеряемом количестве гармоник сигналов автогенераторов.

Как уже указывалось ранее, выводы «опасный сигнал отсутствует» или «модуляция опасным сигналом не обнаружена» недопустимы. В этих случаях необходимо проводить расчет «по шумам».

При организации работ следует учитывать, что измерения в области акустоэлектрических преобразований относятся к числу наиболее сложных инструментальных работ. Приходится учитывать очень большое число различных помех, создаваемых самим техническим средством, достаточно сложных и непостоянных во времени процессов, которые могут внести большие погрешности. Сами измерения весьма сложны, требуют значительных затрат времени. До настоящего времени существует единственный автоматизированный комплекс автоматизации этих измерений — «Талис». Однако любой автомат при специальных исследованиях никогда не заменит полностью человека, и поэтому многое зависит от квалификации оператора.

Некоторую иллюстрацию затрат времени и объема работ может дать такой пример. На исследования представлен телевизионный приемник (не видеодвойка) системы SEKAM, который в процессе эксплуатации будет работать в системе коллективного приема программ центрального и местного вещания на 10 точно определенных телевизионных каналах диапазона метровых и дециметровых волн. Известно, что в процессе эксплуатации приема других частотных каналов не предполагается.

При оценке трудозатрат на исследование возможной модуляции колебаний ВЧ сигналов в данном телевизоре следует иметь в виду измерения модуляции на:

- десяти частотах гетеродина и на их гармониках с проверкой наличия модуляции;
- промежуточных частотах изображения и звука и их гармониках на каждой рабочей частоте;
- частотах и их гармониках цветовых поднесущих;
- частоте строчной развертки и ее гармониках;
- частотах и гармониках ШИМ сигнала импульсного блока питания;
- комбинационных частотах (возможных биений между всеми ними) в различных комбинациях;
- возможно, других генераторов и модуляторов.

И все это в условиях достаточно высокого уровня помех, создаваемых работой различных узлов и блоков самого телевизора, не говоря уже о внешних помехах. Вариантов, как видим, достаточно много.

В данном примере частот измерения было несколько больше 1500. Выполнение таких исследований, если их выполнять в полном объеме (а другого просто не дано), может занять не один рабочий день.

Обратим внимание еще на один немаловажный аспект. Как уже отмечалось при рассмотрении области акустики и вибраций, нормированные величины опасных сигналов заданы на границе контролируемой зоны. Достаточно часто встречается вариант, при котором на выходе некого ВТСС, например телефонного аппарата, опасный сигнал несколько превышает норму. Однако нельзя забывать, что до границы контролируемой зоны, т. е. до того места, где потенциальный противник может подключиться именно к этой линии, тянется 50...70 м телефонной пары. Линий без затухания не бывает. При этом совершенно естественно предположение, что опасный сигнал может достаточно ослабнуть для того, чтобы норма была выполнена. И снова мы приходим к необходимости измерить реальное затухание, на сей раз в электрической линии. Необходимо ввести в линию большой тестовый сигнал, в этой же точке измерить его величину. А потом измерить тот же сигнал на другом конце линии.

Какие-то сложности могут быть только при подключении к линии (ввода сигнала в линию и вывода из нее), например к линии электропитания. Необходимо защитить генератор от сетевого напряжения и в то же время создать достаточный тестовый сигнал. Конструкции и схемы таких переходных устройств существуют, и грамотные специалисты в области специальных исследований владеют необходимым оборудованием и умением его применять.

Вопрос, которого необходимо здесь коснуться, это вопрос о выборе частот, на которых должно оценивается реальное затухание.

Естественно, эти частоты должны выбираться из диапазона, в котором присутствует опасный сигнал. В пределе — весь диапазон, установленный регламентирующими документами. А вот шаг пробных частот не регламентирован. Поэтому мы считаем необходимым выбирать его настолько частым, чтобы значения затухания в двух соседних по частоте точках не различались более, чем на 3 дБ. При выполнении этого условия можно быть уверенным, что не пропущены некие участки частот с аномально низким затуханием.

Если в исследованном диапазоне затухание сильно разнится, то для финального расчета нужно либо брать минимальное его значение, либо усреднять его, обычно по среднеквадратичному закону.

Однако реальное затухание сильно зависит от частоты и среды распространения. В области речевых частот, например, километрическое (т. е. на километр длины) затухание телефонной пары с жилой диаметром 0,5 мм в многопарном кабеле на частоте 800 Гц не более

1,5 дБ. В силовых цепях электропитания затухание сигнала речевого спектра оказывается (по результатам проведённых исследований) даже меньшим. Реальные затухания возникают начиная с частот порядка единиц мегагерц.

В ВЧ диапазоне частот затухание низкочастотных (например, телефонных) кабелей также не нормируется и дать предварительную оценку затухания кабеля трудно, но с повышением частоты это затухание сильно растёт.

Надо также иметь в виду, что при распространении ВЧ сигнала даже небольшого уровня вполне вероятно взаимное влияние между кабелем, несущим информацию, и проложенными рядом с ним другими кабелями за счет параллельного пробега. Теория взаимных влияний между отдельными цепями хорошо проработана еще в 30–50 гг. XX века и нет необходимости приводить ее в данном пособии. К услугам заинтересованных специалистов большое количество различного рода пособий, учебников и монографий на эту тему. Необходимо отметить только одно: вероятность перехода ВЧ сигнала на параллельно идущие кабели всегда существует, а ее значение можно оценить только экспериментально. Но для этого потребуется проведение измерений не в одном (влияющем) кабеле, а во всем пучке кабелей, имеющих параллельный пробег с влияющим, часто расходящимся на несколько направлений (например, телефонные, сигнализации, оповещения и ряд других).

Еще одним подвидом специальных исследований в области акустоэлектрических преобразований являются исследования эффективности различных видов систем активной защиты. Достаточно часто приходится это оценивать, особенно в части прямого акустоэлектрического преобразования, т. е. при зашумлении линий. Как правильно измерить сигналы и оценить эффективность систем активной защиты?

В области НЧ АЭП, во-первых, должен быть измерен опасный сигнал в соответствии с методикой *в отсутствии зашумления*. Рассчитано значение эквивалентного сигнала. Отдельно снимается (измеряется) спектр зашумляющего сигнала системы активной защиты в той же линиии, как правило, в той же точке. Точнее — огибающая спектральной плотности. Почему именно спектр, а не интегральное значение во всей заданной полосе частот?

Не так уж редок случай, когда в заданном диапазоне (не столь важно узок он или широк, важен принципиальный подход) огибающая шумового сигнала весьма неравномерна. При этом не исключен вариант, при котором в каких-то частотных интервалах соотношение сигнал/шум будет меньше нормируемого, хотя при использовании интегральных значений все укладывается в норму. Именно поэтому, если

огибающая спектральной плотности шума оказалась заметно неравномерной, нужно либо отдельно рассчитывать соотношения сигнал/шум для разных частотных интервалов, либо подставлять при расчете минимальное значение шума.

В области ВЧ АЭП ситуация с оценкой эффективности САЗ проще. Как указывалось ранее, полоса частот, занимаемая модулированным сигналом (АМ или узкополосная ЧМ/ФМ), не более 6...20 кГц (двойная полоса речевого сигнала). В пределах такой полосы частот, за редким исключением, спектр любого ВЧ генератора шума равномерен. Поэтому достаточно измерения уровня шумового сигнала такой же (или близкой) полосой. Далее просто рассчитывается отношение сигнал/шум. Причём, учитывая малые значения модуляции и, следовательно, малые значения амплитуд боковых частот, достаточные для блокирования канала утечки значения шума достигаются без труда.

И снова приходится указывать, что все принятые допущения и варианты измерений и расчетов должны быть изложены в протоколе.

Еще один канал возможной утечки необходимо рассматривать при проведении специальных исследований технических средств за счет акустоэлектрических преобразований — канал, образуемый за счет паразитной высокочастотной генерации (ПВЧГ) усилительных устройств в широком смысле этого слова. Перечислять все причины возникновения ПВЧГ не имеет смысла — они подробно излагаются в курсе теоретической радиотехники.

В практике проведения исследований по исследованию наличия/отсутствия паразитной высокочастотной генерации встречались случаи, когда причиной появления паразитной ВЧ генерации в усилителях звукового диапазона частот в области 50...200 МГц являлось превышение допустимого уровня примесей в кристалле микросхемы аналогового усилителя.

Специальной методики для определения наличия/отсутствия ПВЧГ при акустическом воздействии на ТС в настоящее время не существует. Поэтому приходится использовать существующую, которая ориентирована на исследование усилителей в составе ТСПИ.

Как правило, усилители должны исследоваться:

- при изменении напряжений питания в пределах допусков, оговоренных технической документацией;
- перегрузкой усилителей по входу и выходу в пределах, ограниченных либо допустимыми нелинейными искажениями (например, в схемах электронных телефонных аппаратов), либо, вообще, режимом, близким к термической устойчивости активных усилительных элементов (транзисторов, микросхем), а также комбинации этих режимов.

Естественно, что многие ТС, поступающие на СИ, не имеют, если так можно выразиться, «открытого» входа, на который может быть подан внешний тест-сигнал (большинство датчиков пожарной и охранной сигнализации, автономные и встроенные блоки питания и многое другое). В этом случае акустическое воздействие на ТС является единственным способом воздействия.

Аналогично методике исследований модуляции колебаний автогенераторов исследования ПВЧГ должны проводиться как в эфире, так и во всех проводах, отходящих от технического средства, включая и цепи питания. Некоторым отличием в методике измерений следует считать то, что исследования ПВЧГ допускается проводить при расположении измерительной антенны (возможно, и отрезком провода определенной длины) практически вплотную к техническому средству. Объясняется это тем, что данный канал утечки относится к ненормируемым и в некотором смысле случайным, в связи с чем исследования квалифицированы только как обнаружение, а не измерения. Как и в предыдущих разделах, отметим, что при исследовании паразитной ВЧ генерации получаемые результаты в очень сильной степени зависят от оператора, его квалификации, знания предмета исследований и общей эрудиции. На этот случай и создать автоматизированную аппаратуру крайне сложно, либо её работа будет занимать несоразмерное время.

5.2.8. Специальные исследования в области ВЧ навязывания (СИ ВЧН)

Рассматривая проведение СИ в этой области, прежде всего, следует знать, что данный ТКУИ (точнее несколько вариантов этого ТКУИ) относится к весьма небольшому числу каналов, которые до настоящего времени не нормированы. То есть не определён и не установлен регламентирующими документами параметр защищённости и не установлено его нормированное значение.

В связи с этим при СИ необязательно применение средств измерений и измерений вообще. Немногочисленные НМД в этой области «привязаны» к применению конкретных моделей приборов, специально разработанных для них.

Вообще-то вполне возможно и использование метода генератора-приёмника, хотя его реализация связана с весьма сложной технологией.

Рассмотрим этот метод чуть подробнее. Суть метода заключается в прямой имитации, моделировании, при помощи стандартных радиоизмерительных приборов процедуры «нападения». Единственное, вполне понятное упрощение заключается в замене реального акустического речевого сигнала сигналом одночастотным, тональным. Схема эксперимента несложна и приведена на рис. 5.52.

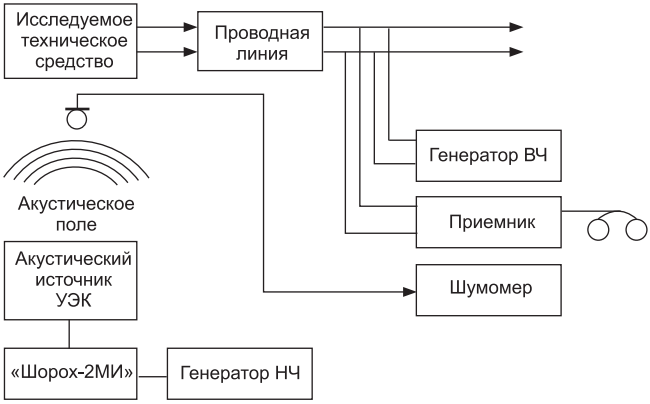


Рис. 5.52. Схема исследования на ВЧ навязывание методом приёмника-генератора

Как видим, схема измерения достаточно похожа на схему СИ при классическом АЭП. В исследуемую линию контактно вводится ВЧ сигнал нормированной величины произвольной частоты в диапазоне частот от 20 кГц до 30 МГц. Одновременно на исследуемое ТС воздействуют акустическим сигналом. Сложность заключается в том, что заранее неизвестны две величины — частота зондирующего сигнала и частота акустического сигнала, на которых может появиться «отклик». Поэтому часто на первом этапе акустическое воздействием заменяют методом стука. То есть слегка постукивают по корпусу исследуемого ТС. Выполнять этот приём и просто и сложно одновременно. Постукивание должно быть частым, несильным и выполняться только диэлектрическим предметом, чтобы не создавать, одновременно, ёмкостных и иных помех. Часто для этого применяют обыкновенный карандаш с вмонтированным ластиком. Применение этого метода обусловлено двумя причинами:

- ударное возбуждение корпуса эквивалентно весьма высокому звуковому давления, порядка 120...130 дБ;
- стук — весьма широкополосное воздействие, таким образом одновременно проверяется воздействие всеми звуковыми частотами.

Если после «прохода» по всему ВЧ диапазону выявились частоты, на которых в приёмнике прослушивается звук постукивания, то на этих частотах выполняют более тщательное исследование уже с акустическим тестовым сигналом.

Основная принципиальная сложность заключается в том, что нужно синхронно перестраивать генератор и приёмник, причём приёмник должен быть расстроен относительно генератора на некоторую частоту. Поясним это на спектрограмме.

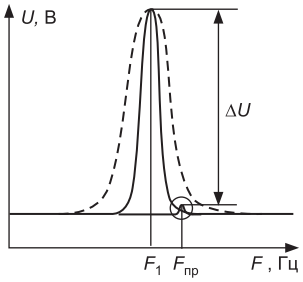


Рис. 5.53. Спектр модулированного ВЧ сигнала. «Боковая» частота заключена в кружок

Как видно на рис. 5.53, сигнал генератора всегда занимает некоторую конечную полосу частот. Ширина этой полосы обусловлена как фазовыми шумами генератора, так и конечной полосой пропускания приёмника (анализатора спектра). Сигнал боковой частоты практически всегда приходится «отыскивать» на фоне скатов полосы сигнала генератора. Это означает, что генератор должен иметь малые фазовые шумы, а приёмник — узкую полосу пропускания с высокой селективностью. В противном случае принять боковую частоту будет невозможно (случай с более «расплывшейся» полосой сигнала генератора показан штриховой линией). При этом приёмник должен быть расстроен относительно генератора на величину, равную воздействующему акустическому сигналу (обычно 1...4 кГц, меньшие значения расстройки реализовать сложнее). Разность между амплитудами сигнала генератора и сигнала боковой частоты обычно от 90 до 40 дБ. Измерить столь малый сигнал «вблизи» столь большого не самая простая задача, требующая средств измерения с высокими параметрами и мастерства оператора.

Как следует из вышеизложенного, метод приёмника-генератора вполне реализуем, но трудоёмок, сложен и очень зависит параметров от применяемых средств измерения.

Более прост метод исследования с применением специализированных приборов. В настоящее время таких приборов на рынке доступно несколько моделей — «Арфа», «Арфа-М», «Арфа-МД» «Облако-2», «Вепрь». Все эти изделия действуют по одному и тому же алгоритму, воздействуя на исследуемое ТС зондирующим сигналом и принимая ответный модулированный сигнал. В каждом из названных приборов тем или иным способом приняты меры по разделению зондирующего и отражённого модулированного сигнала.

Рис. 5.54. Система «Арфа-МД»

Прибор «Арфа-МД» (рис. 5.54) состоит из трех основных блоков: блока управления (БУ), построенного на основе планшетного компьютера, блока формирования и демодуляции сигналов (БФД), блока автономного электропитания (БП).

Связь между блоком управления и блоком формирования и демодуляции сигналов производится по USB-интерфейсу. При включении блока управления напряжение на интерфейсной линии автоматически включает в блоке питания напряжение питания БФД.

Управляющая программа БУ обеспечивает пользовательский интерфейс управления изделием, контроль его работоспособности и выполняет необходимые операции для анализа данных измерения и формирования отчета проведения измерения. Кроме того, управляющая программа задает режимы функционирования и параметры сигналов для блока БФД, а также следит за состоянием аккумуляторов БП.

БФД содержит тракт формирования сигнала ВЧ навязывания с регулировкой мощности выходного сигнал, демодулятор на основе синхронного гетеродина с возможностью подстройки фазы сигнала гетеродина, тракт НЧ фильтрации и усиления, детектор качества демодулированного сигнала.

Демодулируемый ВЧ сигнал выделяется в согласующем устройстве тракта формирования сигнала и, по сути, является аддитивной смесью сигнала ВЧ навязывания и ВЧ сигнала, отраженного от исследуемой нагрузки. В зависимости от режима демодуляции синхронный гетеродин подстраивается по фазе под демодулируемый ВЧ сигнал на прием сигнала синфазного (режим АМ), квадратурного (режим ФМ), или подстраивается по критерию наилучшего качества демодуляции — адаптивный демодулятор. В режиме адаптивного демодулятора фаза гетеродина устанавливается по критерию наилучшего качества слышимости тестового акустического сигнала.

Для настройки наилучшего качества демодулированного сигнала в ручном режиме имеется возможность изменения мощности сигнала ВЧ навязывания и регулировки усиления тракта НЧ.

Блок автономного электропитания обеспечивает работоспособность изделия за исключением БУ (у планшетного компьютера собственный источник).

Имитатор параметрического микрофона служит для проверки работоспособности изделия и соединительных кабелей в полосе частот от 2 до 180 МГц, а также проведения обучения оператора изделия.

Схема имитатора допускает его подключения к цепям постоянного тока с напряжением до 100 В.

Имитатор действует на принципе модуляции проводимости. Модулирующим элементом имитатора параметрического микрофона является полевой транзистор с изолированным затвором. Сопротивление канала транзистора изменяется электрическим сигналом, генерируемым пъезодинамиком, который работает в режиме микрофона.

Изделие имеет следующие режимы проведения исследования:

Рис. 5.55. Общий вид системы «Вепрь»

- ручной режим — проведение исследования методом ВЧ навязывания непосредственно оператором;
- автоматический режим — изделие проведет автоматический поиск каналов утечки при воздействии тестового акустического сигнала;
- анализ помех — режим формирования маски частотных каналов с высоким уровнем шума для ускорения режима автоматического поиска;
- поиск активных источников — режим порогового обнаружения частотных каналов с высоким уровнем сигнала.

Методика работы с данным прибором достаточно подробно изложено Руководстве пользователя. Для общего представления о возможностях «Арфы-МД» вполне достаточно выше изложенного материала, а следующий прибор это система «Вепрь».

Система «Вепрь» (рис. 5.55) предназначена для выявления и исследования опасных сигналов в проводных линиях, возникающих за счет акустоэлектрических преобразований в оконечных устройствах. Исследование осуществляется методом ВЧ навязывания. При этом система «Вепрь» способна выполнять этот поиск в автоматическом режиме. Она включает в свой состав канал формирования тестового акустического сигнала и канал его измерения.

По заданию, сформированному оператором, система «Вепрь» последовательно изменяет частоту зондирующего сигнала и на каж-

дой зондирующей частоте воздействует на исследуемое ТС заданным рядом акустических частот. Все результаты записываются в файл и, по окончании цикла, генерируется технический отчёт. На частотах, на которых система обнаружила модулированный отклик, можно прослушать сигнал модуляции. Система «Вепрь» имеет сертификат ФСТЭК России.

5.2.9. Специальные исследования в области ВЧ облучения (СИ ВЧО)

Специальные исследования в области ВЧО выполняются в соответствии с принципами, весьма сходными с ВЧН. Разница заключается только в способе подачи зондирующего сигнала и приёма отражённого. Вместо гальванического подключения к линии, отходящей от исследуемого ТС, применяется облучение при помощи соответствующей антенны.

Этот ТКУИ также является ненормированным, в силу чего отсутствует установленный параметр защищённости, наличие паразитной модуляции в отражённом сигнале определяется «на слух».

Так же, как и в ВЧН, возможно использование метода приёмника-генератора и специализированных приборов.

Схема исследования для метода приёмника-генератора рассмотрена в разд. 2.5.4 (см. рис. 2.49).

Всё описанное для организации исследования аналогичным методом канала ВЧН верно и для ВЧО. Усложнением является необходимость ещё и выбора размещения излучающей и приёмной антенн, причем на каждой частоте зондирующего сигнала отдельно. Приходится учитывать ещё и неизвестные направления переизлучения (отражения) сигнала от исследуемого ТС. В целом, учитывая количество неизвестных варьируемых параметров, исследования канала ВЧО ещё более кропотливы и длительны.

Из числа специализированных приборов можно назвать системы «Ревиз» и «Омега-А». Оба устройства управляются ПЭВМ и могут работать в автоматизированных режимах. Связь управляющей ПЭВМ с основным блоком устройства осуществляется по USB-кабелю. ПЭВМ осуществляет управление генератором ВЧ и приемником. Зондирующий сигнал в диапазоне частот 30...5000 МГц формируется генератором ВЧ. В комплексе «Ревиз-5000» реализована возможность выбора двух схем работы: с использованием одной приемопередающей (встроенной) антенны; с двумя внешними (приемной и передающей) антеннами.

При работе с одной антенной зондирующий сигнал с выхода генератора через усилитель мощности и направленный ответвитель передается на встроенную широкополосную направленную антенну и излу-

чается в окружающее пространство. Отраженный сигнал принимается той же антенной и через другой выход направленного ответвителя поступает на вход приемника. Направленный ответвитель обеспечивает разделение зондирующего и принимаемого сигнала.

При работе с двумя внешними (приемной и передающей) антеннами зондирующий сигнал с выхода генератора через усилитель мощности передается на внешнюю передающую широкополосную направленную антенну и излучается в окружающее пространство. Отраженный сигнал принимается приемной широкополосной направленной антенной и поступает на вход приемника. Подключение внешних широкополосных антенн осуществляется посредствам разъемов. Приемник перестраивается синхронно с генератором и служит для выделения модуляции принимаемого сигнала. С выхода «(21–11304 Гц)» сигнал модуляции в диапазоне 21...11304 Гц поступает на ПЭВМ и УНЧ. Выход «АНАЛИЗАТОР» служит для подключения внешнего анализатора спектра для анализа модулирующего сигнала в диапазоне частот 0...1000 МГц.

УНЧ служит для вывода сигнала модуляции на головные телефоны и имеет регулятор «ГРОМКОСТЬ». У изделия «Омега» раздельные антенны и более широкий рабочий диапазон частот зондирующего сигнала. Антенны размещаются на штативах, основной приборный блок в отдельной укладке.

Подробное описание приборов было дано во второй главе настоящего издания.

5.2.10. Специальные исследования в области защиты цифровой информации (СИ ЭВТ)

Эта область также весьма обширна и в регламентирующих документах относится к виду разведки и группе каналов утечки через побочные излучения и наводки (ПЭМИН).

Как указывалось ранее, через побочные излучения может происходить утечка различной информации. Однако в этом разделе мы сосредоточимся именно на цифровой, т. е. той информации, которая в виде, цифровых кодов циркулирует в узлах, блоках, устройствах и линиях, в первую очередь средств вычислительной техники, обрабатывающих закрытую информацию, т. е. эксплуатируемых в качестве основных технических средств (ОТСС).

Что и как искать (методологические основы). Для лучшего понимания вопроса рассмотрим основы теории, без понимания которых невозможно представить себе, что именно, какие побочные излучения следует ожидать от некого обобщенного сигнала в цепях ПЭВМ.

Необходимо вспомнить, что задача потенциального противника состоит в том, что он должен решать простейшую задачу о том, что

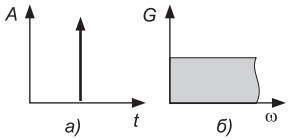


Рис. 5.56. Дельта-функция и ее спектр

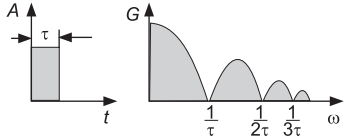


Рис. 5.57. Однократный импульс конечной длительности и его спектр

же передавалось в данный момент, «ноль» или «единица», т. е. бинарная задача решается для одного двоичного разряда. При этом предполагается, что потенциальный противник точно знает структуру устройства, алгоритм обработки информации, виды кодирования и т. д. Вот исходя из этого, и будет рассматриваться модель сигнала и ее предполагаемый спектр.

Простейший одиночный импульсный сигнал, так называемая дельта-функция, приведен на рис. 5.56,*а*. Такой сигнал характеризуется бесконечно малой длительностью и бесконечной амплитудой, а площадь такого импульса всегда равна 1. Спектр такого сигнала приведен на рис. 5.56,*б*, он сплошной (без учета свойств случайных антенн в конкретном техническом средстве), бесконечный по частоте и его огибающая плоская.

Необходимо четко помнить, что в реальности таких импульсов не бывает. Приблизим модель к реальности и рассмотрим одиночный импульс конечной длительности (рис. 5.57). При этом сигнале огибающая спектра стала неравномерной. На рисунке она представлена по абсолютной величине. В реальности каждый четный лепесток направлен во второй квадрант. Такого рода огибающая спектра описывается простым выражением

$$G = U\tau\frac{\sin x}{x}.$$

Изменения вида спектра обусловлены взаимодействием энергий переднего и заднего фронтов импульса во входном устройстве узкополосного анализатора, с помощью которого и строится спектр.

Далее рассмотрим бесконечную последовательность импульсов конечной длительности, что позволит в дальнейшем более реально построить модель. Такой сигнал и его спектр приведены на рис. 5.58.

Необходимо обратить внимание на то, что амплитуда импульсов меньше, чем одиночного импульса на предыдущем рисунке, а амплитуды гармонических составляющих спектра даже выросли. Это не случайное нарушение масштаба, поскольку это только качественное отражение реальности. Это свойство спектра импульсной последовательности лежит в основе существующих методов СИ.

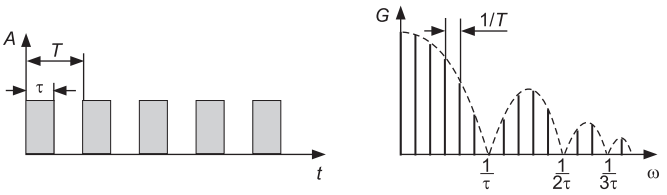


Рис. 5.58. Спектр бесконечной последовательности импульсов

Таким образом, спектр последовательности импульсов становится «линейчатым», сохраняя огибающую одиночного импульса («лепестки» огибающей, по-прежнему, имеют «ширину» $1/\tau$)

$$|E_n| = 2A\frac{\sin(n\omega\tau/2)}{\pi n}.$$

Причем шаг гармоник по частоте обратен периоду следования импульсов. А вот амплитуда гармонических составляющих выросла. Именно этот эффект и позволяет резко улучшить соотношение сигнал/шум при измерении сигналов ПЭМИН.

Все приведенные выше примеры спектров иллюстрируют предельно идеализированную картину. Реальные спектры ПЭМИН при совпадении частот составляющих с теорией имеют абсолютно случайные распределения амплитуд. Необходимо помнить, что реальное излучение является композицией большого числа излучателей (случайных антенн), каждый из которых имеет свою амплитудно-частотную характеристику со своими пиками, провалами, резонансами и т. д.

Необходимо особо отметить следующее. В физическом смысле этих процессов есть одна особенность, по сути, это практически всегда; инженер уверен, что именно такой спектр существует реально, объективно. Мы привыкли априори считать, что наши приборы отражают реальную, объективно существующую картину мира. А ведь это не всегда является истиной. В данном случае «видно» отображение объективной реальности узкополосным селективным прибором. И эти частотные составляющие, гармоники, возникают только в нашем средстве измерения.

В реальности существует только сплошной спектр от каждого фронта каждого импульса. Он конечен, что естественно, поскольку конечна длительность фронта, при этом спектр неравномерный, поскольку искажен свойствами реальных случайных антенн. Но всегда сплошной. За счет инерционности, т. е. своеобразной «памяти» входного устройства, он становится линейчатым только в нашем приемнике и нигде иначе.

В реальных устройствах импульсные последовательности не бывают бесконечными. Практически без исключений любая пересылка,

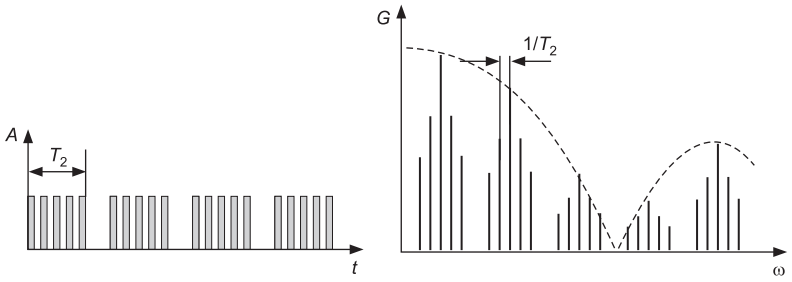


Рис. 5.59. Спектр последовательности пакетов импульсов

обработка и т. д. выполняется пакетами. Поэтому наиболее реальной моделью сигнала в цепях ПЭВМ будет последовательность таких пакетов, в которых длина пакета существенно больше длительности одного импульса. Такая модель и ее спектр представлены на рис. 5.59.

Спектр последовательности пакетов импульсов, изображенный на рис. 5.59 (масштаб изображений для наглядности изменен и приведены не все боковые составляющие), позволяет сделать вывод о том, что около каждой спектральной составляющей, обусловленной самими импульсами, появились боковые составляющие, обусловленные частотой следования пакетов.

Для иллюстрации рассмотрим, например, типовой случай — ПЭМИН видеоподсистемы ПЭВМ. Стандартный тест-режим для СИ этого устройства — это вывод на экран видеосигнала, который представляет собой чередование прямоугольных импульсов с такими же по времени промежутками между ними (сигнал типа «меандр»). Каждая строка растра будет представлять собой пакет импульсов. Число импульсов в пакете равно половине разрешения экрана по горизонтали (для режима 1024×768 это составит 512 импульсов). Затем пауза, обусловленная обратным ходом строчной развертки, и новый пакет.

На рис. 5.60 показан участок спектра такого сигнала. В левой части экрана одна из гармоник тактовой частоты следования импульсов, правее первая и вторая верхние боковые частоты с шагом, равным частоте строчной развертки дисплея.

Данный элементарный пример является одним из самых наглядных, но при этом он и самый простой. Многие сегодняшние виды ПЭМИН гораздо сложнее при анализе.

Исходя из вышеизложенного, становится понятным, сколь важен режим функционирования исследуемого блока (узла) ПЭВМ. Учитывая, что в составе любого цифрового устройства одновременно работают десятки схем, узлов, блоков, без точного знания того, какие именно частоты нужно искать, проведение СИ невозможно. Каждый из сотен сигналов подчиняется некой тактовой частоте. Эти частоты,

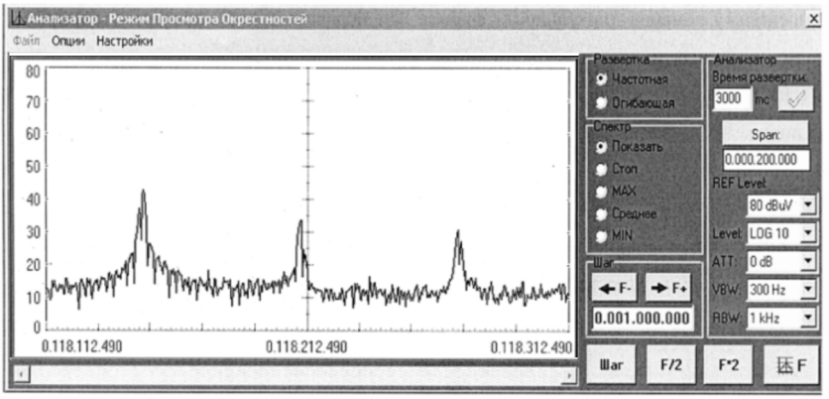


Рис. 5.60. Спектр опасного сигнала от видеоподсистемы. Скрин с экрана системы «Сигурд»

как правило, независимы, многие из них делятся и умножаются. И, к сожалению, все они излучают.

Для выделения опасного сигнала необходимо однозначное знание трех параметров: длительности импульса, частоты их следования в пакете, частоты следования пакетов. Кроме вышеизложенного, следует напомнить, что это же необходимо еще и для правильного расчета результатов измерений.

Вновь обратим внимание на то, что амплитуды гармонических составляющих для последовательности импульсов значительно больше, чем амплитуда огибающей спектральной плотности для одиночного импульса.

Так как нормами определен расчет параметров защищенности одного импульса, независимо от предыдущих и последующих, то в расчетных формулах присутствует операция деления на корень из частоты следования импульсов. Таким образом, при неверном определении этой частоты однозначно получим неверный результат исследования.

Следовательно, частота следования импульсов во время измерений должна быть постоянной. Если тактовая частота во время измерений претерпевает изменения, то:

во-первых, «сдвигаются» со своих мест (по частоте) гармонические составляющие (что же тогда мы будем измерять?);

во-вторых, какую частоту необходимо подставлять при расчете?

Так как объем настоящего курса не предоставляет возможности подробнее рассмотреть все аспекты организации тест-режима (или выбора из имеющихся рабочих режимов устройства) исследуемой ПЭВМ, ограничимся результирующим утверждением о том, что выбранный режим должен обеспечивать прохождение по информацион-

ным цепям бесконечной (или достаточно длительной по времени) последовательности пакетов импульсов с постоянной тактовой частотой и длительностью (как импульсов, так и их пакетов).

Все перечисленные параметры необходимо знать (или измерить в соответствующих цепях) с достаточной для последующего расчета точностью.

5.2.11. Специальные исследования побочных электромагнитных излучений и наводок

Будем рассматривать особенности этого вида специальных исследований дальше. Как уже упоминалось выше, в составе ПЭВМ одновременно функционирует очень большое количество зависимых и независимых устройств. В каждом из них, наряду с информационными, циркулирует большое количество служебных сигналов, тактовых частот и т. д. Необходимо очень точно представлять себе, какие именно сигналы нас интересуют.

Исходя из формулировки задачи перехвата следует, что наибольшую опасность представляет излучение тех устройств, в которых защищаемая информация циркулирует в виде последовательного кода. Фактически, примерно с 1983 г. цепи с параллельным кодированием и разрядностью выше восьми просто не рассматриваются как опасные по каналу ПЭМИН.

В составе достаточно типовой ПЭВМ подпадают под понятие устройств с последовательным кодированием:

- видеоподсистема (включая внутренние интерфейсы мониторов);
- накопители на жестком дисках (включая внешние) и их интерфейсы (некоторые узлы);
- устройства CD, CD-R, CD-RW; DVD, DVD-RW (некоторые узлы);
- устройства внешней флеш-памяти;
- клавиатура;
- последовательные порты COM, IEEE1394, USB;
- принтеры (некоторые узлы).

Особенности этих устройств с точки зрения их специальных исследований уже рассматривались в главе 4.

Действующие в настоящее время нормативные документы обязывают проводить стендовые (лабораторные) СИ для всех устройств, входящих с состав комплекта ПЭВМ и во всех возможных режимах работы, но эти требования обязательны только для выделенных помещений, в которых циркулируют и обрабатываются материалы, составляющие гостайну. При этом объём таких СИ может оказаться весьма большим. Единственной возможностью сокращения объёма работ является право заказчика определить и указать конкретные режимы, в которых будет эксплуатироваться то или иное устройство.

Основное содержание работ. Как и ранее, рассмотрим общий состав работ по специальным исследованиям в привязке к рекомендуемому тексту протокола.

Название организации — лицензиата, выполнившей специальные исследования, ссылка на его лицензии и название объекта специальных исследований.

Цель исследований и контроля, вид исследований. Указывается, что является целью специальных исследований (стендовые СИ с целью определения R_2, r_1, r_1' или оценка защищенности (измерения и расчёт значений Δ), оценка эффективности системы активной защиты).

Место проведения специальных исследований. Как и в области специальных исследований акустоэлектрических преобразований, важно указывать, где проводились исследования: на объекте по месту эксплуатации или на стенде.

Вид проводимого инструментального контроля. Аттестационные или текущие, периодические измерения.

Состав исследуемых устройств и их режимы работы. Необходимо включить в таблицу все устройства из состава исследуемой ПЭВМ или другого объекта информатизации. Обычно в отдельный подраздел включаются средства защиты (если они есть).

Подробное указание моделей и заводские номера всех устройств, входящих в состав комплекса и установленных в системном блоке, не обязательно, если проводились специальные проверки и системный блок опечатан соответствующей голограммой. Однако их упоминание (перечисление) необходимо. Сегодняшние регламентирующие документы требуют *обязательного измерения каждого устройства* комплекса технических средств ПЭВМ. И не только каждого устройства, но каждого устройства во всех режимах его работы, которые могут использоваться при эксплуатации.

Важной особенностью сегодняшних требований является проверка во всех возможных режимах. Ограничить этот список может только заказчик работы, причём письменно.

Контрольно-измерительная аппаратура. Требования к этому разделу такие же, как и при любых других специальных исследованиях. Если применялся автоматизированный комплекс, указывается его заводской номер и сертификат Гостехкомиссии. Если комплекс поверялся как единая система — достаточно привести одно свидетельство о поверке.

Методика проведения специальных исследований. Один из самых важных разделов. Именно здесь подробно излагаются все условия измерений. Разумеется, никто не требует переписывать типовую

методику. Однако все то, о чем говорилось выше, должно быть изложено здесь.

Краткие ссылки на примененные методики и нормы. Какие именно устройства исследовались (желательно с обоснованием, если это не типовой набор), причем отдельно по каждому виду исследований. Описание тест-программ (тест-режимов) для каждого исследованного устройства. Если этого требовали условия проведения специальных исследований, то указываются конкретные параметры размещения антенн (и передающей, и приемной) при измерениях методом реальных зон. Отдельно описываются условия исследований в линиях электропитания. Если оценивалась эффективность систем активной защиты, то каких именно, в каком диапазоне.

С одной стороны, этот раздел должен составляться так, чтобы любой специалист в области специальных исследований (не только представитель контролирующей инстанции, но и просто коллега), прочитав его, смог, не задавая вопросов, однозначно повторить все измерения. С другой стороны, чтобы была полностью понятна логика принятых решений.

Анализ построения системы электропитания и заземления ПЭВМ. Раздел полностью аналогичен такому же разделу при проведении специальных исследований акустоэлектрических преобразований. И цель его та же. Краткое, но исчерпывающее описание системы электропитания и заземления, однозначным выводом из которого следует: нужно ли вообще и что именно в них исследовать.

Результаты измерений и расчетов. Основной раздел. Здесь размещаются таблицы результатов измерений и расчетов. При необходимости — пояснения к конкретным измерениям, схемы размещения АФУ по отношению к исследуемым техническим средствам, фотографии.

В начале раздела обычно приводятся те данные, которые не требуют объемных таблиц. Перечисления тех устройств, данные измерений по которым не приводятся с обоснованием причин. Излагаются общие принципы размещения измерительных антенн, мест подключения пробников и т. д.

Для тех устройств, специальные исследования которых проводились ранее, необходимо указать параметры опасного сигнала (длительность импульса, тактовую частоту) в тех режимах, в которых проводились исследования.

Здесь же могут быть помещены краткие пояснения к построению нижеследующих таблиц.

Далее размещаются таблицы. Перед каждой таблицей должно быть указано: к какому устройству относятся данные, в каком режиме и что именно измерялось. В конце таблицы рекомендуется давать

краткий вывод о том, выполняется или нет условие защищенности. Учитывая, что, как правило, таблицы содержат достаточно много данных, промежуточных результатов расчетов, рекомендуется давать к таблицам расшифровки принятых обозначений.

Выводы. В этом разделе в сводной форме приводится общий вывод о защищенности объекта в целом.

Средства измерения. Основным средством измерения в этой области является селективный измерительный прибор необходимого диапазона частот. В настоящее время это диапазон от 10 кГц до почти 2 ГГц. Приборов, перекрывающих весь такой диапазон, уже вполне достаточно, хотя они недёшевы. А их параметры у относительно недорогих моделей не так высоки, как хотелось бы. Стандартная, принятая во всем мире нижняя частота универсальных анализаторов спектра и измерительных приемников составляет 9 кГц.

Упоминавшиеся ранее приемники FSM уже совсем выходят из употребления, современные приборы отечественного производства («Риап-1,8», приборы серии «Белан») обладают не столь высокими параметрами и удобством применения, как хотелось бы. Чаще всего применяют анализаторы спектра и измерительные приёмники различных зарубежных производителей.

В общем-то все, что было сказано о средствах измерения в разделе АЭП, сохраняет свою силу и здесь, так как задачи во многом одинаковы.

Особо следует упомянуть низкочастотный диапазон (<10 кГц). Несмотря на то что этот диапазон находится за пределами, рассматриваемыми сегодняшними регламентирующими документами, измерять в нем приходится. Как правило, теми же вольтметрами Unipan, которые уже упоминались. Равно как и любыми аналогичными. Однако это приборы измерения эффективного значения сигнала, а методика требует измерения пикового значения. В отсутствии соответствующих приборов все молчаливо согласились «закрыть глаза» на это несоответствие и измеряют эффективное значение (в диапазоне от 10 Гц до 10 или 100 кГц). Разумеется, если точно известна скважность импульсов опасных сигналов, то можно по эффективному значению рассчитать пиковое.

Для измерений на объектах (оценки защищённости) необходимы генераторы сигналов, перекрывающие установленный диапазон, для измерений реального затухания. Однако к этим генераторам есть одно специфическое требование. Для таких измерений крайне важны генераторы с достаточно мощным выходом, которые способны при работе на излучающую антенну создать сигнал, достаточный для его уверенного приема на границе контролируемой зоны при проведении измерений методом реальных зон. Из приборов общего назначения

это Г4-154, Г4-143, Г4-144, Г4-76 и аналогичные. В качестве излучающей антенны для специальных исследований методом реальных зон очень удобна и эффективна антенна от приемников AOR типа DA3000.

Весьма нелишним будет хороший электронный частотомер, качественный широкополосный осциллограф и множество всяких мелочей. Очень полезным будет набор кабелей и переходников, позволяющих подключаться и производить измерения непосредственно в цепях ПЭВМ. Такой комплект разработан и выпускается, хотя сейчас номенклатура кабелей и их параметров в нём уже недостаточна.

Кроме всего перечисленного, в области специальных исследований цифровой техники созданы и эксплуатируются ряд автоматизированных систем (комплексов). В настоящее время сертификаты Гостехкомиссии России имеют комплексы «Зарница-П», «Навигатор», «Легенда», «Сигурд» и АРК-Д1Т1.

Дадим краткую характеристику этим комплексам.

«Зарница-П» (рис. 5.61) — единственный комплекс, созданный на базе нестандартного средства, предназначен для автоматизации измерений при проведении специальных исследований и контроля технических средств ЭВТ с целью определения возможности съема информации со средств вычислительной и оргтехники. «Зарница» обеспечивает измерение параметров побочных электромагнитных излучений (ПЭМИ), обработку результатов измерений, выполнение необходимых расчетов и выпуск отчетной документации при проведении исследований и контроля технических средств ЭВТ. Применение комплекса повышает достоверность и эффективность проведения исследований за счет автоматизации процессов измерения, выявления информативных сигналов, обработки полученных результатов в соответствии с действующими нормативно-методическими документами, выпуска отчетной документации, что снижает трудозатраты на проведение подобных исследований.

Рис. 5.61. Комплекс для исследований ПЭМИН «Зарница-П»

Рис. 5.62. Комплекс для исследований ПЭМИН «Навигатор-ПЗГ»

Его основой является сканирующий приемник серии AOR. В силу этого вопрос его применимости вызывает некоторые сомнения. Существуют оценки метрологических организаций, показывающие нестабильность результатов. Тем не менее, комплекс имеет метрологический сертификат и сертификат Гостехкомиссии РФ. «Зарница» не опознает самостоятельно опасный сигнал на фоне других сигналов, а работает на принципе сравнения излучения в двух режимах исследуемого устройства с выключенным и включенным тест-режимом. Остальное должен делать оператор.

Переносной комплекс «Навигатор-ПЗГ» (рис. 5.62), выполненный на базе анализатора спектра Aerjflex 2399C, предназначен для автоматизации измерений при проведении исследований и контроля технических средств ЭВТ с целью определения возможности съема информации со средств вычислительной и оргтехники. Диапазон частот комплекса 1 кГц...3 ГГц. Программно-аппаратный комплекс серии «Навигатор» обеспечивают: автоматический, автоматизированный, экспертный поиск и обнаружение ПЭМИ (побочные электромагнитные излучения) тестируемой аппаратуры; измерение частоты и пикового значения амплитуды найденных сигналов; «ручную» верификацию списка обнаруженных ПЭМИ и наблюдение в осциллографическом режиме демодулированного тестового сигнала с одновременным прослушиванием теста в звуковом диапазоне частот; исследование систем активного пространственного ВЧ зашумления; определение значения реального затухания электромагнитного поля при проведении аттестационных испытаний объектов информатизации; хранение, обработку и представление результатов поиска и измерений для расчета зон разведдоступности ПЭМИ и коэффициента защищенности объекта в соответствии с утвержденными методиками ФСТЭК России; проведе-

Рис. 5.63. Комплекс «Легенда-05М»

ние инженерных исследований специальных технических средств (радиостанций, радиомикрофонов, систем съема информации и т. д.).

Программно-аппаратный комплекс позволяет: в автоматизированном режиме обнаруживать ПЭМИ тестируемой аппаратуры и формировать список обнаруженных ПЭМИ с регистрацией частоты, уровня ПЭМИ, полосы пропускания и антенн, при которых производилось обнаружение; в автоматизированном режиме верифицировать список обнаруженных ПЭМИ при включенном и выключенном тесте на исследуемой аппаратуре; отображать на мониторе компьютера спектры обнаруженных сигналов; проводить ручную верификацию списка обнаруженных ПЭМИ, используя осциллографический режим работы анализатора для наблюдения демодулированного тестового сигнала с одновременным прослушивания теста в звуковом диапазоне частот; проводить обработку полученных результатов и расчет зон разведдоступности ПЭМИ и коэффициента защищенности объекта в соответствии с утвержденными методиками Гостехкомиссии России; проводить инженерные исследования специальных технических средств (радиостанций, радиомикрофонов, систем съема информации и т. д.).

Два комплекса, построенные на анализаторах Agilent Technology и R&S («Легенда») и IFR («Сигурд»), отличаются тем, что способны самостоятельно опознавать опасный сигнал по форме их огибающих, заданных соответствующими тест-программами.

Комплекс «Легенда-05М» (рис. 5.63) предназначен для проведения специальных исследований на побочные электромагнитные излучения и наводки (ПЭМИН) технических средств обработки информации. Комплекс создан на базе современных приборов ведущих производителей радиоизмерительной аппаратуры Agilent Technologies, Rohde Schwarz. Комплекс работает под управлением специального программного обеспечения, разработанного на основании действующих

нормативно-методических документов ФСТЭК России. Комплекс сертифицирован по требованиям безопасности информации в системе сертификации ФСТЭК России.

Комплекс является автоматизированной системой оценки защищенности средств вычислительной техники от утечки информации по каналу побочных электромагнитных излучений и наводок. Он позволяет осуществить полный цикл работ по инструментальному исследованию технических средств, включая поиск и обнаружение информативных составляющих побочных излучений и наводок, измерение их параметров, а также расчет показателей защищенности технических средств и формирование протокола исследований в соответствии с требованиями нормативно-методического документа ФСТЭК России «Сборник методических документов по контролю защищенности информации, обрабатываемой средствами вычислительной техники, от утечки за счет побочных электромагнитных излучений и наводок» (ФСТЭК России, 2005 г.).

В комплексе предусмотрены: возможность автоматизированного (без участия оператора) обнаружения, распознавания (определение принадлежности к исследуемому техническому средству) и измерения уровней сигналов или полуавтоматизированного (с участием оператора) обнаружение и измерение уровней сигналов технических средств; обработка результатов измерений и расчет зон возможного перехвата ПЭМИН, затухания в линиях; формирование протокола измерений и передача его в Microsoft Office Word для коррекции и вывода на печать.

Система «Сигурд» (рис. 5.64) создана на базе спектроанализатора фирмы IFR (MARCONI), стандартного IBM-совместимого персонального компьютера (настольного или Notebook) и комплекта ан-

Рис. 5.64. Система «Сигурд»

тенн. Комплекс может включать в свой состав спектроанализторы аналогичного класса и других производителей при условии доработки программного обеспечения. Могут быть применены любые антенны, предназначенные для работы в диапазоне от 9 кГц до 2 ГГц.

Рекомендуется применение активных широкополосных антенн. Параметры антенн (антенный коэффициент) вводятся в управляющую программу и учитываются автоматически при выборе соответствующей антенны. Замена антенн в процессе измерений осуществляется оператором в соответствии с сообщениями управляющей программы. Основным отличием данной системы от аналогичных разработок является четырёхэтапное обнаружение и измерение сигналов и полностью автоматическое адаптивное распознавание частот (сигналов) ПЭМИН среди всех, присутствующих в эфире, и автоматическое дистанционное управление параметрами тест-режимов на исследуемой ПЭВМ (на базе типового IrDA канала). На первом этапе выполнения задания в автоматическом режиме осуществляется фильтрация всех входных сигналов по энергетическому критерию (превышение на заданную величину над уровнем шумов). Возможно применение цифровой фильтрации, включая вейвлет-преобразование. Далее система выполняет коррекцию каждого выявленного сигнала, уточняя его частоту. На третьем этапе осуществляется корреляционный двухступенчатый анализ сигналов в сравнении их с эталоном, хранящимися в файловой библиотеке. Эталон сигнала синтезируется оператором по спектрограмме реального сигнала в процессе формирования задания. Предусмотрено выделение сигналов, корреляционные характеристики которых не позволяют программе сделать однозначный вывод, и выдача их на экран оператору для принятия решения. На последнем этапе выполняется измерение выявленных опасных сигналов. Для опасных сигналов, огибающая (спектрограмма) которых не может быть «окрашена» при помощи соответствующего теста-режима, предусмотрен режим работы с предварительно создаваемой базой сигналов (при остановленном тесте или выключенном исследуемом устройстве). В этом случае система регистрирует и измеряет только те сигналы, которые отсутствуют в базе. Выполнение расчёта результатов (вызов модуля расчёта) может выполняться как вручную, так и автоматически. В последнем случае все результаты измерений передаются в модуль расчёта без участия оператора.

Учитывая сложный характер спектра ПЭМИН, предусмотрен дополнительный режим просмотра ближайших частотных «окрестностей» любого выявленного сигнала с целью обнаружения боковых частот. Система автоматически вычисляет шаг гармоник ПЭМИН, их боковых частот и может вести анализ на основе выявленной сетки

частот, что ещё больше сокращает затраты времени и повышает надёжность результатов.

Все спектры, зафиксированные в процессе СИ, могут быть сохранены для последующего анализа и сравнения с любыми другими. Данная функция позволяет, кроме того, вести анализ спектров методом «наложения», при котором сравниваются два спектра, снятых в разных режимах работы исследуемого устройства. Изменения спектра по сравнению с сохранённым при наложении выделяются цветом.

Управляющая программа позволяет управлять всеми необходимыми режимами работы спектроанализатора. Все задаваемые оператором параметры запоминаются в виде задания. Библиотека заданий сохраняется для последующего использования, в том числе любое задание может быть использовано в последующем без изменений или с любыми изменениями. Выполнение любого задания может быть приостановлено оператором в любой момент и продолжено или запущено сначала или продолжено с изменёнными в случае необходимости параметрами.

Предусмотрен и ручной режим работы со спектроанализатором с управлением всеми функциями спектроанализатора от компьютера. Спектроанализатором можно управлять и автономно с помощью его органов управления. При возврате под управление компьютера оператор может продолжить выполнение задания с параметрами, предусмотренными заданием или с введёнными с пульта управления спектроанализатора вручную.

В состав системы входит в виде самостоятельного программного модуля задача расчёта требуемых параметров исследуемых устройств. Исходными данными для расчёта являются результаты измерений ПЭМИН исследуемого устройства в виде файла данных и дополнительные данные, вводимые оператором. Результатом расчёта является таблица данных измерений и расчётов, предназначенная для включения в отчёт по СИ, формируемый в любом текстовом редакторе. Модуль реализует стандартный метод расчёта.

Спектроанализатор и рекомендуемые модели антенн включены в Госреестр измерительных приборов и поставляются с калибровочными сертификатами и свидетельствами о поверке.

Спектроанализатор имеет возможность непрерывной работы с автономным электропитанием до полутора часов, что позволяет в ряде случаев минимизировать уровень помех при измерениях. Рекомендуемые измерительные антенны также предусматривают автономное электропитание. Таким образом, при использовании компьютера Notebook, весь комплекс может быть мобильным и автономным.

Так же примерно функционирует и комплекс АРК-Д1Т1, выполненный на базе собственной разработки панорамного приёмника фир-

мой «Иркос». Данный комплекс позиционируется разработчиком как комплекс радиомониторинга, одной из опций которого является проведение СИ.

Особенности специальных исследований ПЭМИН. Существуют две основные методики оценки защищенности технических средств от утечки по каналу ПЭМИН. Это методика собственно специальных исследований, результатом применения которой является определение значений R_2, r_1 и r'_1 (стендовые, лабораторные СИ), и методика оценки защищенности, результатом которой является измеренное и рассчитанное соотношение сигнал/шум на границе контролируемой зоны.

Обе методики обязательны к применению, но ареал их применимости различен.

Методика стендовых СИ предназначена для обязательной начальной оценки спецсвойств всех ОТСС, предназначенных для обработки информации на объекте. Эти исследования проводятся на стандартизованных измерительных площадках, соответствующих требованиям ГОСТ Р 51320. Таким образом, появилась возможность сопоставления результатов измерений, выполненных разными лицензиатами. Рассчитанные по результатам измерений значения R_2 и r_1 позволяют спроектировать построение системы защиты, обоснованно сделать вывод о применении средств зашумления.

Вторая методика позволяет получить отношение сигнал/шум на границе КЗ объекта, которое рассчитываетсяна основании измерений реального затухания сигналов. Эта методика предназначена для оценки защищённости объектов, в ее рамках не определяются значения R_2, r_1 и r'_1.

Как уже указывалось ранее, специалист (оператор), проводящий СИ, приступая к измерениям, должен уже более чем наполовину знать, что именно ему должны показать приборы. Возможно, такое утверждение звучит парадоксально, но это именно так. Иначе работа либо затянется на неопределенный срок, либо будет выполнена на недостаточном уровне. Все, что касается параметров опасного сигнала, должно быть известно абсолютно точно.

Столь же твердо оператор должен знать набор действий, которые он обязан предпринять, если опасный сигнал не выявляется в типовых условиях измерения. От самых простейших (типа придвинуть антенну поближе), до самых изощренных (снять на время стенку системного блока, заменить кабель на неэкранированный или кабель с заранее внесенной асимметрией). Только убедившись, что опасный сигнал существует и его составляющие «стоят на своих местах», можно делать вывод о том, что значения опасных сигналов ниже уровня шумов

и именно поэтому не выявляются при нормированных условиях измерения.

Кроме того, точность определения и установки частоты различных средств измерения различна. Предположим, что тактовая частота некого сигнала измерена непосредственно в цепи устройства цифровым частотомером и оказалась равна 38,4694 МГц. Настроив приемник или анализатор спектра на эту частоту, часто можно обнаружить, что эта же частота, но измеренная другим прибором, равна 38,4705 МГц. При узкой полосе пропускания приемного устройства можно и «промахнуться».

Размещение антенн относительно исследуемого объекта — один из самых критичных параметров. Мало того, что надо найти вокруг устройства («по сфере») место, где сигнал имеет наибольшую величину, но и проверить при этом ориентацию диполя или рамки в пространстве для получения именно максимальных значений сигнала. А в разных частях диапазона эта ориентация может быть и различна. То же самое касается размещения токового трансформатора на кабеле питания.

Единственно правильное решение в этом случае — проверить варианты размещения АФУ на всех частотах существования опасных сигналов и выполнять измерения на каждой частоте «по максимуму», как и предписывает методика. Это не вызывает затруднений при работе вручную. А при работе автоматизированных комплексов приходится разбивать весь диапазон исследования на отдельные поддиапазоны, измерения в которых выполняются при различных положениях АФУ.

И опять не лишне напомнить, что все это должно быть отражено в протоколе.

При этом для экономии времени крайне полезно знать, какую компоненту — электрическую или магнитную — следует ожидать. Для этого необходимо однозначно представлять себе, какие компоненты технического средства являются излучателем (случайной антенной). От катушки с током (печатающая головка матричного принтера) не приходится ожидать хоть сколько-нибудь заметной электрической компоненты, а от видеоподсистемы — магнитной. Во всяком случае, в нормированном для магнитной компоненты диапазоне частот. Исключения бывают, но весьма редко. А вот струйный принтер, к сожалению, требует измерения по каждой из компонент электромагнитного поля.

Можно отметить, что для установленного диапазона частот (до 30 МГц) по магнитной компоненте поля расстояния до 1,5...2 м являются много меньшими длины волны (10 м). Поэтому поле в этой зоне носит квазистатический характер и не связано с электрическим через

волновое сопротивление пространства. Следовательно, электрическая и магнитная компоненты существуют независимо друг от друга.

Очень важным вопросом бывает вопрос электропитания и заземления средств измерения при специальных исследованиях.

В линиях электропитания исследуемых ОТСС, как правило, наличествует опасный сигнал и порою весьма заметный. Если активная антенна или сам измерительный прибор питается от этой же сети, то этот опасный сигнал может попасть на вход. Причем с неизвестной фазой. Ошибка легко может составить до десятков дБ. Даже если эти линии (электропитания) разные, но лежат в одном кабельном канале, то для частот в десятки–сотни мегагерц эффект может заметно проявиться. Есть различные способы проверки, имеет ли место погрешность за счет такого эффекта, и проводить эту проверку следует неукоснительно. То же самое можно сказать и о заземлении. Все проверяется опытным путем в процессе работы до начала собственно измерений. Весьма часто приходится применять автономное электропитание и другие способы (заземление на разные системы, отказ от заземления измерительного комплекса, правильное размещение составляющих измерительного комплекса и т. д.).

Исходя из тех теоретических основ, которые были изложены в начале раздела, можно предположить, что опасные сигналы могут появляться только на тактовых частотах и их боковых частотах. Это вполне справедливо и правильно. Однако не очень часто, но четко выраженные опасные сигналы появляются на совершенно «незаконных» частотах. Это можно объяснить работой паразитных генераторов (возбуждением каких-то электронных компонентов), частота возбуждения которых модулирована опасным сигналом. Есть довольно надежный прием, позволяющий предположение превратить почти в уверенность. Если эта частота присутствует и при остановленном тесте (уже без «окраски») и, особенно, если она не слишком стабильна, «ползает» по частоте, то это почти наверняка, паразитная генерация. Но основное не это. Как требуют регламентирующие документы, паразитных возбуждений быть не должно. А это значит, что оператор обязан внимательно и не торопясь просмотреть *весь* установленный диапазон. Вот где становится незаменимой автоматика! Человеку, увы, свойственна невнимательность, особенно после многочасового сидения за приемником.

И, кстати, почти всегда возникает вопрос — а что измерять? Исходя из самых «начальных» регламентирующих документов измерять нужно все сигналы, имеющие признаки информативности.

Отсюда вопрос — что же такое «признак информативности»? Вопрос далеко не прост и сегодня. Попробуем сформулировать ответ.

Это сигналы, амплитуда которых претерпевает изменения при изменении обрабатываемой (пересылаемой, записываемой и т. д.) информации. Здесь необходимо отметить, что именно информации, а не служебных команд, заголовков пакетов и т. д. И еще очень важно подчеркнуть — *амплитуда*.

Представим себе, что в некой цепи пересылается в последовательном коде бесконечная последовательность байтов FF (т. е. в двоичном коде 11111111). Есть вполне реальная тактовая частота и длительность импульса. Метод кодирования — последовательный импульсный код, единица кодируется наличием импульса, ноль — отсутствием. Пауза между соседними импульсами равна длительности импульса.

Изменим пересылаемый байт, например, на 10101010. Совершенно понятно, что изменилась тактовая частота следования импульсов, она упала в два раза. Возможно даже и скорее всего изменится и амплитуда частотных составляющих. Но для наблюдателя (приемника), «видящего» одну конкретную частоту (для нечетных гармоник), ее амплитуда упадет до нуля, сигнал просто исчезнет. Можно ли такой случай рассматривать как изменение амплитуды? Нет, механизм здесь совсем иной. Именно поэтому так важно точно знать, что «делает» тест-программа. И правильно ее «сконструировать».

Как правило, наиболее однозначно истолковываемыми являются такие тесты, которые обеспечивают старт-стопный режим работы. В этом случае места для эффектов, подобных вышеописанному, не остается.

В качестве примера приведен результат работы тест-программы «Сигурд-Тест» в режиме исследования видеоподсистемы. При этом видеосигнал на экране монитора исследуемой ПЭВМ представляет собой «картинку», приведенную ниже. В каждой строке растра чередуются черные и белые элементы изображения — пиксели. Каждому прямоугольному импульсу на рис. 5.65 соответствует одна серая полоса на рис. 5.66, 5.67. Группе из 5 полос — один кадр развертки. Уровни шумов в промежутках между импульсами — это время пауз в работе теста (промежутки между серыми полосами). Более длительный промежуток в конце каждого кадра облегчает распознавание опасного сигнала как оператору, так и блоку распознавания системы.

Итак, есть набор «честных» сигналов в неком диапазоне частот. Амплитуды их очень различны. Все ли измерять? Вопрос не праздный, каждое измерение — это время, и немалое.

Здесь следует исходить из следующих принципов. В соответствии с методикой параметры защищенности рассчитываются в частотных полосах «шириной» $1/\tau$. Следовательно, разобьем вопрос на две части. Все ли «лепестки» и все ли сигналы в пределах лепестка измерять?

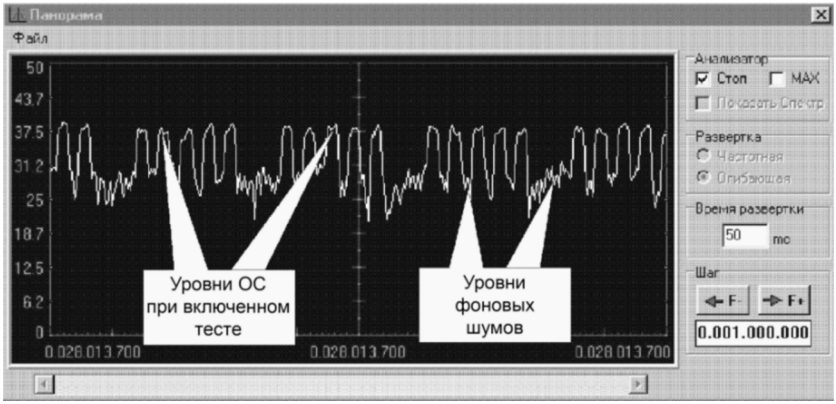


Рис. 5.65. Огибающая сигнала ПЭМИН видеоподсистемы ПЭВМ при загруженном тесте. Скрин с экрана системы «Сигурд»

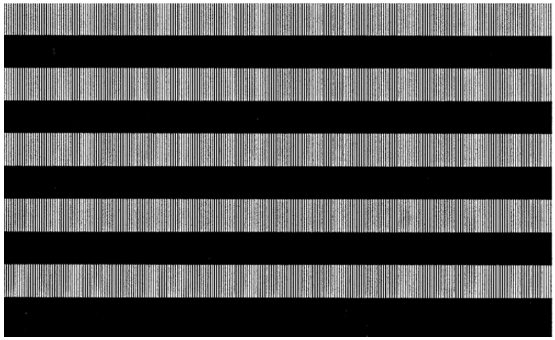


Рис. 5.66. Вид теста видеоподсистемы в режиме «пиксель через пиксель» на экране монитора исследуемой ПЭВМ. Скрин с экрана исследуемой ПЭВМ

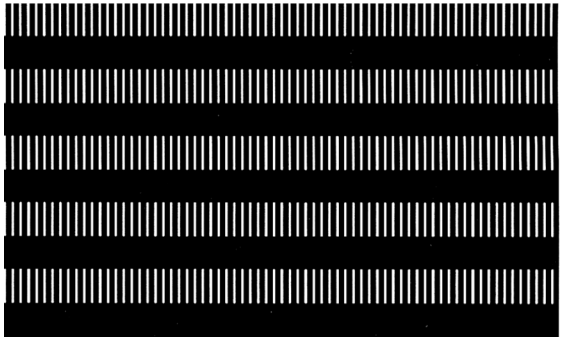


Рис. 5.67. Вид теста видеоподсистемы в режиме «5 пикселей через 15 пикселей» на экране монитора исследуемой ПЭВМ. Скрин с экрана исследуемой ПЭВМ

На первую часть вопроса ответ однозначный — в общем случае все. Если «рядом» находятся несколько лепестков, наиболее опасным при одинаковом значении ОС является более высокочастотный лепесток. Это верно до частот порядка 60 МГц, на более высоких частотах (выше 100 МГц) такая закономерность «меняет знак» и менее выражена.

Со второй частью вопроса чуть сложнее. Если в некотором лепестке имеется n сигналов разной амплитуды, то надо помнить, что первой операцией их математической обработки является вычисление значения

$$\sqrt{\sum E(\rho H)^2_{c,i}}.$$

Из выражения следует, что сигналы с наибольшими амплитудами являются определяющими. Те сигналы, которые меньше самого большого на 12...15 дБ практически не вносят хоть сколько-нибудь заметного вклада. Причем от их количества уже почти ничего не зависит (разумеется, в разумных пределах, если таких «малышей» десятки, то их нельзя не учитывать). Подтверждением правильности такого подхода является «Методика оценки защищенности...», в которой все основано только на самом большом сигнале в лепестке или на сигналах, меньших самого большого не более чем в 2 раза (−6 дБ).

Особенности измерений реальных затуханий. Достаточно часто возникают определенные затруднения при измерениях реального затухания сигналов. Собственно говоря, это уже описанный метод учета реального затухания в канале, только применительно к каналу утечки через ПЭМИН. Как и всегда, при таких измерениях необходимо ввести в канал тест-сигнал большого уровня, позволяющий надежно измерить его значение на дальнем конце канала, т. е. на границе КЗ.

В соответствии с методикой излучающая антенна должна быть установлена на месте технического средства, защищенность которого оценивается. Разумеется, не надо понимать это буквально как догму. Вполне достаточно, чтобы антенна была размещена вблизи технического средства. В общем случае расстояние между антенной и техническим средством должно быть значительно меньше, чем расстояние от антенны до границы контролируемой зоны, точнее — до той точки, где будет размещаться приемная антенна.

Излучающая антенна, крайне желательно, должна быть ненаправленной, хотя бы в горизонтальной плоскости. Иначе достаточно сложно имитировать ПЭМИН исследуемого технического средства. Именно поэтому рекомендуется применение (см. выше, раздел «Средства измерения») антенны DA3000. Данная рекомендация относится к случаю измерения реального затухания для электрического поля. Если решается задача измерения затухания для магнитной

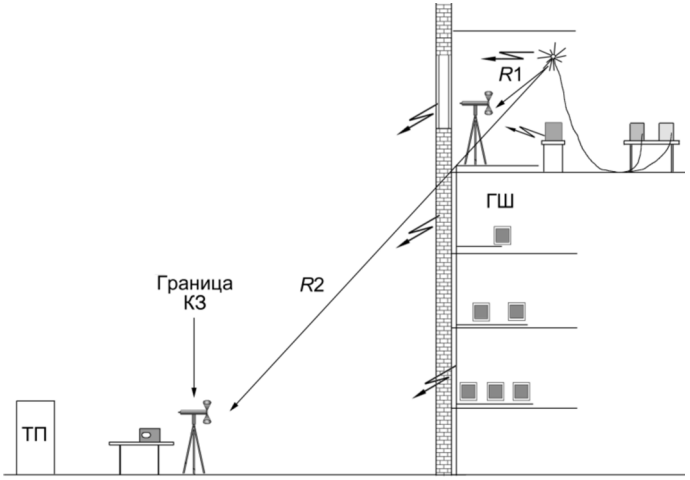


Рис. 5.68. Схема измерений методом реальных зон

компоненты, то единственная излучающая антенна (как, впрочем, и приемная) — это рамка с током. Это нестандартное оборудование, и его придется изготавливать.

В помещении, где расположен защищаемый объект ЭВТ, излучающую антенну рекомендуется размещать на том же расстоянии от внешней стены, окна, что и исследуемое техническое средство. Это связано с тем, что чаще всего в современных зданиях из сборного железобетона основной путь электромагнитной волны к границе контролируемой зоны — это оконный проем и переизлучение металлоконструкциями стены. В меньшей степени, но в общем случае присутствует и излучение линий электропитания.

Общая схема измерений приведена на рис. 5.68. Как видно из схемы, напряженность поля на границе контролируемой зоны представляет собой суперпозицию многочисленных излучателей. Особое внимание нужно обращать на электропитание приборов при этих измерениях. Зачастую генератор ВЧ может выдавать весьма заметный сигнал в эту цепь. В результате этот сигнал, во-первых, может по той же линии электропитания попасть в приемную антенну или в сам приемник. Результаты измерений будут искажены. Вообще, в данном случае гораздо надежнее автономное электропитание и антенны, и приемника. При его отсутствии необходима тщательнейшая проверка отсутствия связей по питанию и устранение их при наличии.

Если граница контролируемой зоны расположена в нескольких местах примерно на равных расстояниях от исследуемого технического средства, то измерения должны быть проведены во всех этих местах. В практике нередки случаи, когда затухание сигнала при его

прохождении через объем здания получается меньшим, чем на таком же расстоянии в свободном пространстве. Видимо, «работают» на переизлучение какие-то случайные антенны.

Отдельно следует рассмотреть вопрос о сетке частот, на которых необходимо производить измерения. В соответствующей методике указано, что эти измерения должны производиться «на частотах опасного сигнала». Однако, как было показано выше, реальный опасный сигнал имеет практически всегда сплошной спектр.

Выбор соответствующего алгоритма не так прост. Если производить измерения на частотах опасного сигнала при тест-режиме исследуемого устройства, то какое отношение эти частоты имеют к реальным рабочим режимам? К тому же зачастую частоты тестового опасного сигнала весьма далеко отстоят друг от друга по частоте, следовательно, затухание в промежутках между ними просто не будет оценено.

Более логично опираться на спектр ПЭМИН при реальной работе. Как было отмечено выше, спектр однократного импульса всегда сплошной. Можно было бы исходить из того, что на частотах в середине каждого лепестка огибающей спектральной плотности сигнал максимален. Но эта теоретическая огибающая очень искажена характеристиками случайных излучателей. Таким образом, единственным разумным подходом являются измерения реального затухания для каждой частотной полосы $1/\tau$, т. е. для каждого лепестка, в котором присутствует ПЭМИН.

В каждом лепестке должно быть взято столько пробных частотных точек, чтобы они достаточно гладко описывали кривую изменений значений затухания (обычно не более 10...20 точек). В диапазоне более низких частот следует ожидать большей изрезанности огибающей и, следовательно, необходим меньший шаг пробных частот.

При разбросе реальных затуханий в лепестке не более 6 дБ можно брать его минимальное значение. При большем разбросе (сильной изрезанности огибающей) пользоваться критериями, примененными в соответствующей методике по расчету эффективности системы активной защиты (сама задача вычисления уровня сигнала системы активной защиты в лепестке практически совпадает с рассматриваемой). Допустимо, с нашей точки зрения, рассчитывать среднеквадратичное затухание.

Автоматизация измерения реального затухания, учитывающая все перечисленные особенности процесса измерений, не слишком простая задача. Однако на сегодняшний день и она решена системой «Стентор» (рис. 5.69). Эта система обеспечивает выполнение измерений как в эфире, так и в линиях в полностью автоматическом режиме. При этом мощность излучения тестового сигнала подбирается

Рис. 5.69. Система «Стентор»

автоматически, «по минимому» загрязняя эфир. Система полностью совместима с системой «Сигурд», являясь её расширением. Результаты измерений реального затухания автоматически передаются в программу расчёта «Сигурд-Дельта» и учитываются в соответствии с действующей методикой.

В тех случаях, когда на границе контролируемой зоны не удается принять тестовый сигнал из-за значительного его затухания и спадания ниже уровня шумов, в расчет реального затухания следует подставлять сами шумы. Обычно при применении достаточно чувствительных приемников рассчитанного таким образом реального затухания бывает достаточно. В этих случаях оператор должен быть абсолютно уверен, что сигнал не принимается именно вследствие его малости, а не по другим причинам. Такая ситуация достаточно часто встречается при размещении защищаемых технических средств ниже уровня первого этажа (цокольный этаж, подвал) и на частотах ниже 10 МГц. В последнем случае причина, в основном, заключается в неэффективности излучающей антенны на низких частотах и, как следствие, низкого уровня тест-сигнала. Каких-то общих рекомендаций для решения этой проблемы привести не представляется возможным, к счастью, измерения реального затухания ПЭМИН на таких низких частотах достаточно редки.

Оценка эффективности САЗ. Последним, о чем стоит упомянуть, являются специальные исследования ПЭМИН в части оценки эффективности системы активной защиты.

Вопрос немаловажный, поскольку это один из основных методов защиты по каналу ПЭМИН для средств ЭВТ. До последнего времени

никаких ограничений (по мощности помехи) в его применении не было, однако с 24.06.2002 г. в соответствии с Решением ГКРЧ № 19/5 установлены предельные уровни излучения генераторов шума для защиты средств ЭВТ. Позже вышли новые документы ГКРЧ (Решение ГКРЧ № 05-10-03-001 от 28.11.2005 г., Протокол 05-10 и Постановление Правительства РФ № 539 от 12 октября 2004 г.) и установлены предельные уровни шума на нормированных расстояниях от генератора, методы измерения и контроля (Нормы 8-95 и ГОСТ Р 51320-99) и т. д.

Следует иметь в виду, что в соответствии с Постановлением Правительства РФ № 539 владельцы генераторов шума обязаны зарегистрировать их в местных органах связьнадзора.

Правда, есть и нестыковки в этих документах. Так, регламентирующими документами ФСТЭК диапазон излучения генераторов зашумления установлен почти до 2 ГГц, а Решения ГКРЧ устанавливают диапазон до 1 ГГц. Эти разночтения приводят, порою, к спорным ситуациям при официализации активных средств защиты.

Упомянутые ограничения приводят к тому, что с некоторой степенью приближения можно утверждать, что ПЭВМ, которая требует по результатам специальных исследований радиуса R_2 более 50 м, почти наверняка для своего зашумления потребует от системы зашумления уровней, перекрывающих нормы ГКРЧ.

Каков же общий алгоритм выполнения специальных исследований в этой области?

Вначале проводятся обычные специальные исследования защищаемой ПЭВМ, затем выполняются измерения электромагнитного сигнала от системы активной защиты (естественно, как и для опасного сигнала — раздельно, по электрической и магнитной компонентам поля). Так же, как и при измерении реального затухания, основная «единица» по частотной шкале — это полоса шириной $1/\tau$.

В соответствующей методике указано, что эти измерения должны производиться полосой измерительного приёмника с таким же шагом по частоте. Таким образом, в полосе, например, 100 МГц необходимо выполнить 833 измерения (при полосе приёмника 120 кГц). Вручную такое требование выполнить нереально, на это способны только автоматизированные системы, такие как «Сигурд». Система «Сигурд» выполняет такие измерения в диапазоне частот от десятков МГц до $\approx$1 ГГц, максимум за 7...10 мин, не более. И не допускает при этом никаких ошибок. Причем вместе с обработкой результатов по установленным методикам и расчетом соотношений сигнал/шум.

Как правило, антенна (антенны) системы активной защиты размещаются вблизи защищаемой ПЭВМ, если же их, по тем или иным причинам, необходимо разместить подальше, то желательно, чтобы

в направлении минимального расстояния до границы контролируемой зоны антенны системы активной защиты размещались ближе к границе, чем ПЭВМ. Если же таких направлений не одно, то решать придется на месте по результатам исследований. Впрочем, при большом запасе по уровню сигнала системы активной защиты это особой роли не играет. Далее рассчитываются соотношения сигнал/шум в каждом лепестке и сравниваются с нормированными значениями.

Практически так же выполняется оценка эффективности системы активной защиты в линиях, например в электропитании. Действующая методика предлагает использовать для измерения сигналов в линиях пробник. Предписание понятное, ведь пробником измеряется напряжение в линии, а именно в единицах отношения напряжений нормируется отношение сигнал/шум. Однако методика никак не определяет точку измерения. А из-за несогласованности линий для сигналов ВЧ они обычно работают в режиме стоячей волны. Поэтому от точки измерения в решающей степени зависит и результат. К глубокому сожалению, этот вопрос обойдён молчанием.

Собственно, применение токоизмерителя прямо не запрещено. Следует только иметь в виду, что применение токоизмерителя (токового трансформатора) предполагает необходимость знания сопротивления линии на частоте измерения для перевода измеренного значения в напряжение. Зато токовый трансформатор можно установить на кабеле электропитания там, где опасный сигнал имеет наибольшую величину. Обычно в этой же точке измеряется и сигнал системы активной защиты. Наибольшее значение эта рекомендация имеет при измерении опасного сигнала. Учитывая характер сигнала системы активной защиты, эффекты стоячей волны в кабелях электропитания для этих сигналов выражены слабо.

Точно так же можно рассчитывать и защищенность в отсутствии системы активной защиты. Только вместо шумового сигнала системы активной защиты в расчет необходимо подставлять значения нормированных шумов (из соответствующих графиков в нормативных документах). Правда, такой расчет, как правило, дает отрицательные результаты. Если зафиксированы хоть немного выявляющиеся над шумами опасные сигналы, то они практически всегда превышают установленные соотношения сигнал/шум (по отношению к нормированным шумам).

Еще одна особенность проведения специальных исследований касается такого стандартного устройства, как видеоподсистема. Практически всегда (как указывалось в примере выше) при измерениях ПЭМИН видеоподсистемы используют тест «пиксель через пиксель». В этом случае шаг гармоник по частоте имеет самую большую величину. Самих гармоник в результате немного, объем работы уменьша-

ется. Однако вспомним спектр такого сигнала — спектр одиночного импульса. В первом лепестке находится 90 % его энергии. А при таком тесте получается, что мы пытаемся оценить излучение в этой полосе частот по одной-единственной гармонике. Абсолютно некорректно. Длина волны в этом диапазоне изменяется в десятки раз (как минимум, спектр реального видеосигнала, например, от набранного на экране текста, имеет нижнюю границу частот около 1 МГц). Соответственно очень сильно меняются и свойства случайных излучателей.

В связи с этим в тех случаях, когда рассчитанное для стандартного теста значение R_2 близко к имеющемуся минимальному расстоянию до границы контролируемой зоны, а также для объектов ЭВТ достаточно высокой категории, необходимо проводить измерения и расчеты в первом лепестке в тест-режиме с гораздо более низкой тактовой частотой. При этом в первом лепестке будут находиться несколько частотных составляющих ПЭМИН видеосигнала. Это позволит произвести оценку защищенности гораздо объективнее. В принципе, достаточно снизить тактовую частоту в 5...7 раз (т. е. задать, например, режим «один пиксель через семь»).

Совершенно новую область СИ ПЭМИН составляют исследования получивших широкое распространение цифровых интерфейсов. Это и внешние интерфейсы (USB 2.0, IEEE1394, DVI — точнее TDMS) и внутренние, принадлежащие в первую очередь схемотехнике современных мониторов (RSDS, LVDS, мини LVDS и др.). Рассмотрение их особенностей приведено ранее, однако упомянем, что особенностями ПЭМИН этих интерфейсов является, как правило, широкополосность, достигающая первых десятков МГц, сложность подбора тестового режима, невысокие уровни и высокая информативность этих видов ПЭМИН.

Контрольные вопросы для самостоятельной работы

1. На каких ограждающих конструкциях нецелесообразно применение САЗ?
2. В каких случаях необходимо применение метода измерения реального затухания и в чем его физический смысл?
3. Каковы оптимальные способы размещения излучателей акустической САЗ?
4. Как должен размещаться источник тест-сигнала при вибрационных и акустических измерениях?
5. Какие системы должны быть проанализированы при подготовке к СИ АЭП?
6. Какие каналы утечки информации должны исследоваться при СИ АЭП?
7. Какие физические эффекты приводят к возникновению прямого АЭП (НЧ АЭП)?
8. Как проверить наличие и уменьшить уровень наводок на исследуемое ВТСС в процессе СИ АЭП?
9. Как образуются модуляционные каналы утечки речевой информации?
10. Как должен выглядеть спектр последовательности пакетов импульсов?
11. Каковы основные критерии предварительного анализа ТС перед СИ ПЭМИН?
12. Какие сигналы должны измеряться при СИ ПЭМИН?

13. Каковы основные требования к тест-режиму исследуемого ТС?

14. Назовите организационные меры, которые нужно принять для защиты объекта.

15. Какую цель преследуют поисковые мероприятия?

16. Назовите пассивные и активные методы технической защиты.

17. Перечислите методы защиты речевой информации.

18. Какая разница между звукоизоляцией и вибрационной и акустической защитой помещения?

19. Каким образом нейтрализуются звукозаписывающие устройства и радиомикрофоны?

20. Дайте характеристики устройств защиты оконечного оборудования слаботочных линий.

21. Перечислите способы защиты абонентских телефонных линий.

22. Какова основная цель экранирования?

23. Перечислите основные требования, предъявляемые к устройствам заземления.

24. Сравните защитные свойства сетевых помехоподавляющих фильтров и генераторов зашумления сети питания. Укажите области применения данных изделий.

25. Назовите технические мероприятия защиты информации в СВТ.

26. Перечислите основные критерии защищенности СВТ.

27. Порядок и особенности проведения специальных исследований технических средств ЭВТ.

28. В чем сущность графического метода расчета радиуса зоны II (R_2)?

29. Основное назначение комплексов защиты от несанкционированного доступа.

30. Что такое персональный идентификатор? Какие виды идентификаторов применяются в системах защиты от НСД? Назовите основные свойства идентификатора.

31. Какие процедуры выполняются системой защиты от НСД до момента загрузки ОС?

32. Что выполняется в процессе аутентификации? Какие виды процессов аутентификации применяются в системах защиты от НСД?

33. Чем определяется стойкость процесса идентификации/аутентификации?

34. Что понимается под определением права разграничения доступа?

35. Что понимается под объектом доступа?

36. Как реализуется мандатный принцип разграничения доступа?

37. Какие подсистемы входят в состав средств разграничения доступа?

38. Какие аппаратные ресурсы входят в типовой состав системы защиты от НСД?

39. Какие параметры регистрируются в системном журнале в процессе работы пользователя? Для чего ведется системный журнал?

40. Какие системы защиты от НСД могут применяться в АС, обрабатывающих информацию, составляющую государственную тайну?

Приложение № 1

XXXXXXX Экз. № _____

УТВЕРЖДАЮ
XXXXXXXXX
«_»_____ _____ 2014 г.

ПРЕДПИСАНИЕ
на эксплуатацию средства вычислительной техники
(СВТ)
№156/2014

Москва
2014 г.

Настоящее «Предписание...» определяет порядок размещения, монтаж и эксплуатацию основных технических средств (ОТС), входящих в состав СВТ, размещаемого в помещении № 4016, по адресу: _____ и предназначенных для обработки и хранения информации, имеющей гриф «_____».

«Предписание...» разработано с учетом:

- «Протокола лабораторных специальных исследований средства вычислительной техники от утечки информации по каналампобочных электромагнитных излучений и наводок» № XXX (мк. XXс от XX.XX.XXXX г.), на основе результатов специальных исследований основного технического средства, проведенных специалистами ООО «XXX «XXXXXXX»;
- «Специальных требований и рекомендаций по защите информации, составляющей государственную тайну, от утечки по техническим каналам» (СТР), Гостехкомиссия России, 1997 г.

1. Состав оборудования ОТС

1.1. В соответствии с действующими нормативными документами по специальным требованиям и в соответствии с результатами лабораторных специальных исследований **разрешается** использовать СВТ в составе:

Таблица 1

Состав СВТ

№	Наименование	Тип, модель	Зав. (сер.) номер
1	Системный блок Midi Tower	Depo Neos 490	083757-030
2	Монитор	RoverScan Optima 171	544FRYI2200429
3	Клавиатура	Defender KM-2501	015100040904
4	Оптический манипулятор «мышь»	Genius NetScroll EYE	110859002641
5	Принтер	HP LaserJet 1022 Q5912A	CNBV5CHJCS

для обработки информации, имеющей гриф «**xxxxxxxxxxxxxx**», при условии выполнения нижеследующих требований.

2. Требования по размещению и монтажу

2.1. Установка оборудования СВТ в помещении постоянной или временной эксплуатации производится в соответствии с техническим паспортом на объект информатизации, настоящим «Предписанием...», инструкцией по эксплуатации и другой эксплуатационной документацией.

2.2. При эксплуатации оборудования СВТ (таблица 1) необходимо обеспечить расстояния, указанные в таблице 2, от СВТ до:

- возможного места размещения стационарных типов средств разведки, большее или равное $R_{2\text{стац}}$;

- возможного места размещения возимых типов средств разведки, большее или равное $R_{2\text{воз}}$;
- возможного места размещения носимых типов средств разведки, большее или равное $R_{2\text{нос}}$;
- сосредоточенных случайных антенн (устройств ВТСС, линии которых выходят за пределы установленной КЗ), большее или равное r_1;
- распределенных случайных антенн (линий выходящих за пределы установленной КЗ), большее или равное r_1'.

Таблица 2

Категория	$R_{2\text{стац}}$, м	$R_{2\text{воз}}$, м	$R_{2\text{нос}}$, м	r_1, м	r_1', м
Вторая	35	15	7	2,0	0,6

2.3. Монтаж оборудования ОТС должен выполняться с помощью штатных кабелей из комплекта поставки оборудования, приведенного в таблице 1 настоящего «Предписания...».

3. Требования к электропитанию и заземлению СВТ

3.1. Электропитание СВТ должно осуществляться через сертифицированные (аттестованные) по требованиям безопасности информации сетевые помехоподавляющие фильтры с фильтрацией сигналов в нулевом проводе, либо с использованием систем активного зашумления в соответствии с положениями раздела 9 «Требований и рекомендаций к системе электропитания технических средств и систем» («Специальных требований и рекомендаций по защите информации, составляющей государственную тайну, от утечки по техническим каналам (СТР)», утвержденных Решением № 55 Гостехкомиссии России от 23 мая 1997 г.).

Примечание. Допускается осуществлять электропитание СВТ от ТП, расположенной за пределами КЗ, при условии использования сертифицированных (аттестованных) по требованиям безопасности информации, помехоподавляющих фильтров или систем активного зашумления (САЗ), устанавливаемых на фидерах электропитания 380/220 В, 50 Гц с последующим проведением инструментального контроля специальных параметров специализированной организацией.

3.2. Заземляющее устройство (контур заземления) СВТ объекта информатизации должно находится в единой с СВТ контролируемой зоне и располагаться от границ КЗ и от подземных коммуникаций, имеющих выход за пределы этой зоны на расстоянии не менее 10 м. в соответствии с положениями раздела 10 «Требований к системе заземления технических средств и систем» («Специальных требований

и рекомендаций по защите информации, составляющей государственную тайну, от утечки по техническим каналам (СТР)», утвержденных Решением № 55 Гостехкомиссии России от 23 мая 1997 г.).

Примечание. Допускается в случае невыполнения указанного требования осуществлять заземление СВТ от заземляющего устройства, находящегося за пределами КЗ, при условии использования четырехпроводных помехоподавляющих фильтров с фильтрацией нулевого провода (для случая заземления от глухо заземленной нейтрали), выполнение повторного заземления, разместив заземляющее устройство в пределах КЗ, выполнения разделения заземлений с использованием помехоподавляющего фильтра и разделительного трансформатора, или использование систем активного зашумления, устанавливаемых на заземляющем проводе, с последующим проведением инструментального контроля специальных параметров специализированной организацией.

4. Требования по эксплуатации

4.1. Ввод в эксплуатацию СВТ осуществляется пользователем с привлечением, при необходимости, специалистов специальных служб и оформлением акта ввода в эксплуатацию при условии выполнения требований настоящего «Предписания...» в части п.п. 2.1–2.3 и п. 3.

4.2. При эксплуатации СВТ запрещается:

- размещать и производить перемещение устройств, входящих в состав ОТС, с нарушением требований п. 2.2;
- производить измерения, подключаться к гнездам, работать с открытыми крышками, кожухами во время обработки секретной информации;
- вносить изменения в схему, конструкцию и монтаж СВТ без согласования с организацией, проводившей специальные исследования;
- изменять установленное разрешение видеоподсистемы (1024$\times$ 768, 75 Гц);
- подключать к LPT, USB и COM портам устройства, не входящие в состав СВТ таблицы 1;
- обрабатывать «**совершенно секретную**» информацию при невыполнении требований разделов 2, 3.
- использовать в качестве заземлителей трубопроводы, водоводы и оболочки кабелей, выходящие за пределы КЗ.

4.3. Замена вышедших из строя отдельных функционально законченных блоков ТС (дисплей, системный блок, клавиатура, манипулятор «мышь» и др. из состава СВТ) должна осуществляться на аналогичные, прошедшие специальные исследования и проверку и имеющие равные или меньшие значения размеров зон R_2 и r_1.

5. Контроль за соблюдением требований предписания

5.1. Контроль за соблюдением требований данного предписания возлагается на пользователя СВТ и службу защиты информации эксплуатирующей организации.

5.2. Периодичность контроля параметров СВТ определяется соответствующей службой организации и должна проводиться не реже одной проверки в год.

Начальник лаборатории
специальных исследований Xxxxxxxxxx X.X.

Приложение № 2

Гриф
Экз. № ___

УТВЕРЖДАЮ
Генеральный директор
XXXXXXXX XXXXX XXXXXX
XXXXXXXXX
_____ /X.X. Xxxxxxxx/
_____ 201_г.

ПРЕДПИСАНИЕ
на эксплуатацию вспомогательных технических средств и систем (ВТСС)
XXXXXXXXXXXXXXXXXXXXXXXXXXX
№ XXX/2014

2014 г.

Настоящее предписание разработано на основании требований нормативных документов и результатов специальных исследований ВТСС объекта информатизации xxxxxxxxxxxxxxxxxxxxxxx. Предписание определяет перечень мер и средств, обеспечивающих выполнение требований, предъявляемых к объекту информатизации.

В соответствии с действующими нормативными документами по специальным требованиям и результатам специальных исследований разрешается эксплуатировать ВТСС в выделенном(ых) помещении(ях) первой, второй и третьей категории(й) в составе, приведенном в таблице 1.

Таблица 1

№	Наименование устройства	Тип, модель	Зав. №	Примечания
1	АРМ в составе:			
1.1	Системный блок Hewlett Packard Compaq	D230MT	CZC3421NNF	
1.2	Монитор Hewlett Packard	1502	CNC3350JCO	
1.3	Клавиатура Hewlett Packard Compaq	SDM4700P	B55890 JQAPF04M	
1.4	Манипулятор «мышь» Hewlett Packard	CP-15K	LZB72506610	
1.4	Активные колонки Creative с адаптером Creative, Tamura 628F4303	SBS-300	LKM 02503 9514	
2	Датчик охранный ИК	Ademco9981	Инв. №№ 3674, 3675	2 шт.
3	Датчик пожарной дымовой оптический	Aritech DP2051	б/н	2шт.
4	Кондиционер сплит National с ПДУ	A75c380	CZ-SFINF73353 6000172	
5	Динамик системы оповещения RCF (пассивный) с установленным устройством защиты МП-5	DU-B101	б/н	
6	Системный цифровой телефонный аппарат Ericsson	Dialog3213	Инв. №4533	
7	Телефонный аппарат с автоответчиком Panasonic	KX-T2470B	3JCHD170204	
8	Телевизор Philips с ПДУ	29PT8402	QG1097411020	
9	Видеомагнитофон Philips с ПДУ	VR 967/58	VN0697380011	
10	Сетевой фильтр PilotTENO	Noise Protector	б/н	
11	Абонентский пульт переговорного устройства RCF	BM 8001	Q 96639	
12	Калькулятор Citizen	SDC-839	910603	
13	Аквариум Juwel (без компрессора)	-	2923 (инв.)	
14	Телефонный аппарат правительственной связи	A5-4	32763	
15	Сетевой фильтр Pilot	Power Cube, B	б/н	

№	Наименование устройства	Тип, модель	Зав. №	Примечания
	Средства защиты:			
16	Система виброакустического зашумления с комплектом датчиков	«Шорох-1»	Зав.№1084-032	Сертификат Гостехкомиссии России
17	Устройство защиты	МП-5	Зав. №...	

1. Требования при эксплуатации

1.1. Установка ВТСС в помещении постоянной эксплуатации производится в соответствии с техническим паспортом на объект информатизации (настоящим Предписанием), техническим описанием, инструкцией по эксплуатации и другой эксплуатационной документацией.

1.2. Оборудование АРМ в составе (таблица 1, п. 1) должно размещаться на расстояниях не менее 1,6 м от границ установленной контролируемой зоны.

1.3. К остальным ВТС (таблица 1) требования по размещению в КЗ не предъявляются.

1.4. Оборудование АРМ в составе (таблица 1, п. 1) должно размещаться от другого оборудования ВТС и посторонних линейно-кабельных цепей, имеющих выходы за пределы КЗ объекта, на расстояниях не менее 1,4 м.

1.5. К остальным ВТС (ВТСС), не имеющим выхода за пределы КЗ (таблица 1), требования по размещению в КЗ не предъявляются (допускается размещение их «вплотную без касания»).

2. Требования по эксплуатации в период проведения закрытых мероприятий

2.1. Сигнальный кабель системного блока HP Compag (D230MT) АРМ физически (с видимым разрывом) отключить от абонентской розетки цепи объектовой локальной вычислительной сети (ЛВС).

2.2. Сигнальный шнур системного цифрового телефонного аппарата MD110DBC (662001/901 R9A) физически (с видимым разрывом) отключить от абонентской телефонной розетки УАТС Ericsson.

2.3. Сигнальный шнур телефонного аппарата (с автоответчиком) Panasonic (KX-T2470B) физически (с видимым разрывом) отключить от абонентской телефонной розетки, а его адаптер питания (KX-A11BM) физически (с видимым разрывом) отключить (вынуть из розетки) от сети электропитания 220 В, 50 Гц.

2.4. Все электрическое оборудование (люминесцентные лампы, нагреватель и компрессор) аквариума Juwel (инв. № 2923) физически (с видимым разрывом) отключить от сети электропитания 220 В, 50 Гц.

2.5. На абонентском пульте переговорного устройства RCF (BM 8001) физически (с видимым разрывом) раскоммутировать разъемный соединитель сигнально-питающей цепи, уходящей на станцию.

2.6. К остальным ВТС (таблица 1) требования при подготовке к проведению закрытых мероприятий не предъявляются.

2.7. Проверить и при необходимости заменить автономные источники питания (батареи, аккумуляторы) в устройствах защиты (МП-5 и т. п.).

2.8. Включить кнопку электропитания 220 В, 50 Гц на блоке (системе) защиты «Шорох» и визуально проконтролировать наличие свечения светодиодного индикатора «сеть».

2.9. Исключить возможность визуального просмотра текстовой и артикуляционной закрытой обрабатываемой информации из-за пределов помещения.

2.10. Проведение периодического визуального контроля наличия свечения светодиодного индикатора «сеть» на блоке генератора системы зашумления «Шорох».

ВНИМАНИЕ:

При проведении в ВП закрытых мероприятий ведение телефонных разговоров **ЗАПРЕЩЕНО**.

В случае аварийного (непреднамеренного/преднамеренного) пропадания в ВП электропитающего напряжения 380/220 В, 50 Гц, контролируемого по отсутствию свечения светодиодного индикатора «сеть» генератора шума «Шорох» и отсутствию в ВП специфического акустического шумового сигнала, проведение закрытых мероприятий **ЗАПРЕЩАЕТСЯ** до устранения аварийной ситуации.

3. При эксплуатации ВТСС

3.1. Запрещается:

- размещать и производить перемещение устройств, входящих в состав ВТСС, с нарушением требований п. 1.2;
- производить измерения, подключаться к гнездам, работать с открытыми крышками, кожухами во время проведения закрытых мероприятий (во время обработки секретной информации на ОТСС);
- вносить изменения в схему, конструкцию и монтаж ВТСС без согласования с организацией, проводившей специальные исследования;
- отключать, демонтировать, заменять средства защиты ВТСС без согласования с организацией, проводившей специальные исследования.

3.2. Ввод в эксплуатацию ВТСС осуществляется пользователем с привлечением, при необходимости, специалистов специальных служб

и оформлением акта ввода в эксплуатацию в части выполнения требований п.п. 1.2–1.5.

3.3. Внесение изменений в состав оборудования, а также конструктивных и схемных изменений в блоках ВТСС не допускается.

3.4. Замена вышедших из строя отдельных функционально законченных блоков ТС должна осуществляться на аналогичные, прошедшие специальные исследования и проверку.

4. Дополнительные требования

4.1. Ввод в эксплуатацию оборудования ВТС в выделенном помещении осуществляется по результатам проведенных специальных работ специализированной организацией ХХХ «ХХХХХХ» и оформлением «Акта ввода в эксплуатацию» в части выполнения требований настоящего «Предписания...».

5. Контроль за соблюдением требований предписания

5.1. Контроль за соблюдением требований данного предписания возлагается на пользователя ВТСС с привлечением специалистов специальных служб эксплуатирующей организации.

5.2. Периодичность контроля параметров изделия определяется специальной службой организации, но не реже одной проверки в год.

Начальник лаборатории
специальных исследований X.X. Xxxxxxxxx

Приложение № 3

ПРОТОКОЛ

инструментального контроля выполнения норм

противодействия акустической речевой разведке в помещении

(наименование объекта)

№ XXX/2007

ОБЩЕСТВО С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ

«XXXXXXXXXXXX XXXXXXXXXX «XXXXXXX»

(ООО «XXX «XXXXXXX»)

В январе 201_года специалистами ООО «XXX «XXXXXXX», действующего на основании Лицензии ФСБ России № 6749 и Лицензии ФСТЭК России № 94, в соответствии с Государственным контрактом № XXX/XX проведён инструментальный контроль выполнения норм противодействия акустической речевой разведке по каналу акустики и виброакустики в выделенном помещении (ВП) (наименование объекта).

1. Объект контроля

Объектом контроля является защищаемое помещение ВП № 1234.

2. Вид проводимого инструментального контроля

Проводимый контроль является **аттестационным**.

3. Назначение объекта и его краткое описание

3.1. Категория объекта защиты.

Помещение подлежит защите в соответствии с требованиями норм для X категории объекта защиты, приведенных в разделе 2 «Сборника нормативно-методических документов по противодействию акустической речевой разведке (НМД АРР)», Гостехкомиссия России 2002 г.

3.2. Контролируемая зона

Границей контролируемой зоны объекта является периметр объекта, огороженный забором. Защищаемое помещение не выходит на границу КЗ. Документ, определяющий границу КЗ, — XXXXXX.

3.3. Размещение выделенного помещения.

Помещение расположено в здании по адресу Xxxxxx xxxx xxx и находится на третьем этаже трехэтажного здания. Вокруг здания объекта имеется охраняемая территория, огороженная по периметру забором. Расстояние от здания объекта до забора от 15 до 40 м (15 м — фасадная сторона здания и 40 м — тыльная).

3.4. Граничащие с ВП помещения (расположение помещений считается относительно наблюдателя, стоящего спиной к входной двери):

слева — рабочее помещение № XX;
справа — рабочее помещение № XX;
снизу — рабочие помещения № № XX,XX;
сверху —чердак здания;
спереди — нет, свободное пространство (окно);
сзади — коридор третьего этажа.

3.5. Ограждающие конструкции.

3.5.1. Ограждающими конструкциями ВП являются:

- внешняя несущая стена здания;
- внутренние перегородки, отделяющие ВП от коридора, помещения № 39 и № 37;
- перекрытия потолка и пола.

3.5.2. Внешняя стена выполнена из кирпича. Толщина внешней стены не менее 70 см, штукатурка 20 мм, лист гипсокартона 12,5 мм, обои.

3.5.3. Внутренние перегородки выполнены из двух слоев гипсокартона, обои с обоих сторон. Пустота между плитами гипсокартона (100 мм) заполнена минеральной ватой.

3.5.4. Перекрытия пола и потолка выполнены из стандартных пустотелых железобетонных плит 205 мм, цементно-песчаная связка 40 мм, плиты ДСП 20 мм, демпфирующая прокладка из пенохлорвинила 3 мм, ламинат 8 мм. Фальшпол в помещении отсутствует. Общая толщина перекрытия $\sim$275 мм.

3.5.5. В ВП установлен фальшпотолок из плит 40$\times$40 см из материала типа «Армстронг» на алюминиевом профиле 40$\times$40 мм. Расстояние от плит перекрытия до подвесного потолка около 25 см.

3.5.6. Над ВП расположен чердак здания. Внешний вид чердака представлен на фото 1. На полу чердака уложена цементная стяжка толщиной не менее 4 см.

3.5.7. В перегородке с коридором установлена филенчатая дверь (из наборных досок). Дверь одинарная двухстворчатая, без тамбура. Высота дверных полотен 208 см, ширина 67 см, толщина 2,5 см (по торцу створки). Со стороны ВП есть порог (деревянная накладка) высотой 1,5 см. Зазор между порогом и створкой двери около 0,4 см. По контуру прилегания дверного полотна к дверной коробке проложен резиновый уплотнитель. В местах стыка створок (по центру) установлена накладная планка. Уплотнительный материал в месте стыка створок отсутствует. Общий вид двери со стороны коридора и со стороны кабинета показан на фото 2 и фото 3 соответственно.

3.5.8. В двух проемах наружной стены установлено по одному оконному блоку. Рамы и коробки оконных блоков изготовлены из пустотелого металлопластикового профиля. Остекление выполнено двухкамерными стеклопакетами. Общий вид оконного блока показан

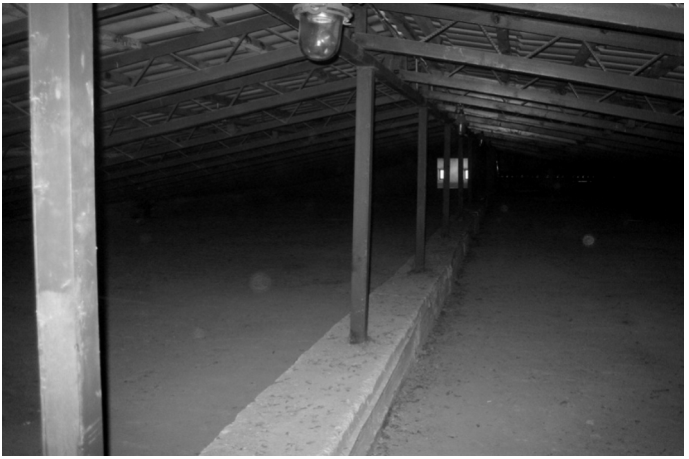


Фото 1. Чердак здания

Фото 2. Входная дверь кабинета № X со стороны коридора

Фото 3. Входная дверь кабинета № X со стороны ВП

на фото 4. Оба окна ВП выходят во внутренний двор объекта. Размеры стеклопакетов (по стеклу) составляют:

верхняя фрамуга — 117,5×40 см;

левая створка — 44×139 см;

правая створка — 44×139 см.

3.6. Инженерно-технические системы.

Фото 4. Окно помещения № X

3.6.1. В ВП имеются следующие инженерно-технические системы:

- система отопления;
- система вентиляции (с принудительной рециркуляцией).

3.6.2. Система отопления.

Снабжение теплоносителем осуществляется от городского ЦТП. Ввод теплоносителя в здание выполнен через подвальное помещение, расположенное в торце здания.

В помещении установлены два металлокерамических радиатора отопления. В каждом радиаторе по 6 секций. Подвод труб отопления к радиаторам осуществляется из соседнего помещения (слева). Теплоноситель проходит транзитом по радиаторам отопления ВП в следующее помещение (справа). В противоположных торцах здания проложены стояки (ввод и «обратка») откуда по этажам раздаётся теплоноситель. Разлив по трубам теплоносителя осуществляется горизонтально вдоль всего здания (из одного помещения в другое). Минимальный пробег (погонное расстояние по трубе) от защищаемого помещения № 38 до ввода труб в здание объекта около 33 м.

3.6.3. Система вентиляции.

В ВП имеется только система приточной вентиляции. Системы вытяжной вентиляции нет. По коридору этажа проложен металлический короб (40×15 см), от которого в помещения этажа врезаны отводы (25×15 см). Ближайшее место возможного непреднамеренного прослушивания в кабинете слева (№ XX). Расположение отвода в ВП и кабинет № показано на фото 5.

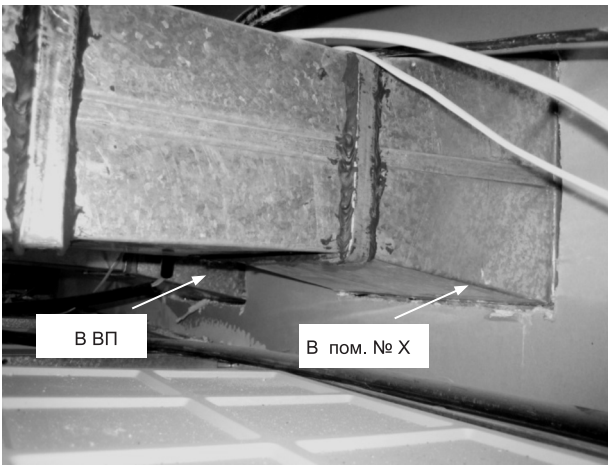


Фото 5. Вентиляционные каналы в ВП и кабинет № X

3.7. Условия речевой деятельности в защищаемом помещении.

3.7.1. В ВП отсутствует система звукоусиления.

3.7.2. Источник речи в ВП не локализован.

4. Контролируемые каналы и возможные направления ведения акустической речевой разведки

4.1. Подлежащие контролю каналы перехвата речевой информации:

- акустический (включая непреднамеренное прослушивание);
- вибрационный.

4.2. По отношению к ВП возможно непреднамеренное прослушивание речи в следующих направлениях:

- из граничащего сзади коридора через дверной блок;
- из граничащего справа помещения № X через перегородку;
- из граничащего слева помещения № X через перегородку;
- из граничащего сверху чердачного помещения через перекрытия потолка;
- из граничащих снизу помещений № X и № Y через перекрытия пола;
- из ближайшего помещения № X через систему вентиляции;
- из ближайшего помещения № X через открытое окно;
- из ближайшего помещения № X через открытое окно.

4.2. По отношению к ВП возможно ведение акустической речевой разведки по вибрационному каналу через трубы системы отопления из-за границы контролируемой зоны.

Примечание. учитывая, что окна защищаемого помещения не выходят на границу контролируемой зоны (окна выходят во внутренний

двор) и что объект не является особорежимным, а также на основании «Программы ...» п. 6.4 (мк. XXX от X.XX.2006), по согласованию с представителями экспертной организации в/ч XXXX, защита остекления окон, рам и внешней стены помещения от дистанционной разведки при помощи лазерного зондирования не осуществлялась.

5. Описание применяемых мер и средств защиты

5.1. Для обеспечения защиты речевой информации в помещении № XX введена в эксплуатацию система активной защиты (САЗ) на базе генератора «XXXXXXX», зав. № XXXXXX.

5.2. Дверной проем в коридор защищен от утечки по акустическому каналу акустическим излучателем OMS-2000, расположенным над дверным блоком со стороны коридора третьего этажа.

5.3. Система вентиляции защищена от утечки по акустическому каналу акустическим излучателем OMS-2000, размещенным в воздуховоде приточной вентиляции (со стороны ВП).

6. Перечень измерительной аппаратуры

6.1. При проведении измерений использовалась следующая контрольно-измерительная аппаратура из комплекта автоматизированной системы оценки защищенности помещений «XXXXX», зав. № ТШ069-04:

- прецизионный интегрирующий шумомер Larson Davis 824A зав. № 2568 с предусилителем PRM902 зав. № 2286;
- измерительный микрофон PCB 130D20, зав. № 17061;
- измерительный микрофон PCB 130D20, зав. № 17063;
- акселерометр АР-98, зав. № 3185;
- калибратор звукового давления CALL 200, зав. № 3591;
- генератор «XXXXX_XX», зав. № МИ089-03;
- акустический излучатель (колонка) «XXXXX_XX», инв. 2145.

Примечание. Вся измерительная аппаратура имеет действующие сертификаты о поверке.

7. Метод проведения измерений

7.1. Измерения, расчет результатов и оценка выполнения норм противодействия проводились в соответствии со «Сборником нормативно-методических документов по противодействию акустической речевой разведке» (НМД АРР), Гостехкомиссия России 2002 г.

7.2. При проведении акустических и виброакустических измерений выбор контрольных точек осуществлялся с помощью предварительных замеров. По предварительным измерениям устанавливалась наихудшая точка, по которой осуществлялась настройка САЗ. В случае, если в направлении измерений не применялась система активной

защиты, в протоколе и приложении приведены точки с максимальными значениями разборчивости из всех измеренных в указанном направлении.

7.3. Контрольные точки приведены в таблице 1.

Таблица 1

Акустические и виброакустические измерения

Исследуемая ограждающая конструкция или элемент ИТС	Обозначение КТ	Норма W
Вибрационный канал		
Система отопления	КТ1...КТ 3	0,X
Акустический канал		
Дверной блок в направлении коридора	КТ4...КТ 6	0,X
Правая перегородка	К7...КТ10	0,X
Левая перегородка	КТ11...КТ15	0,X
Система приточной вентиляции	КТ16	0,X
Перекрытие пола	КТ17...КТ24	0,X
Перекрытия потолка	КТ25...КТ 30	0,X
Окна ВП в направлениях соседнего помещений	КТ31, КТ32	0,X

7.3.1. Контрольные точки по акустическому каналу

Измерения двери и внутренних перегородок проводилось согласно схеме 1.

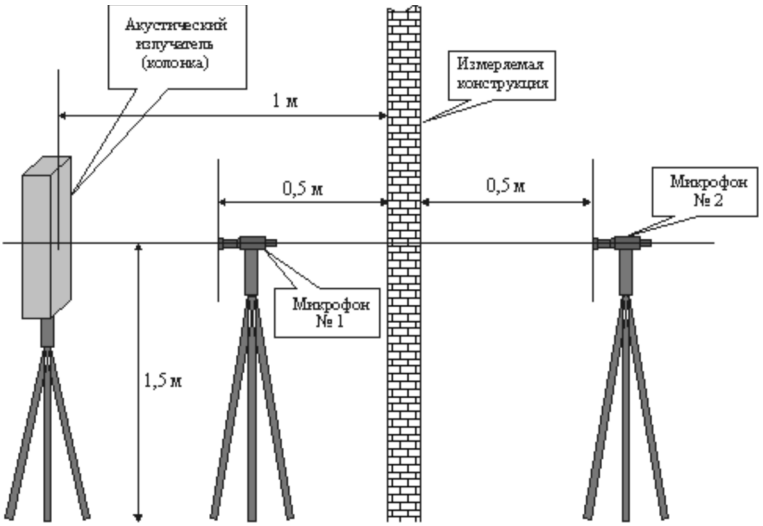


Схема 1. Расстановка микрофонов при измерениях внутренних перегородок и дверей

При измерениях перекрытий пола расстановка измерительных микрофонов осуществлялась согласно схеме 2.

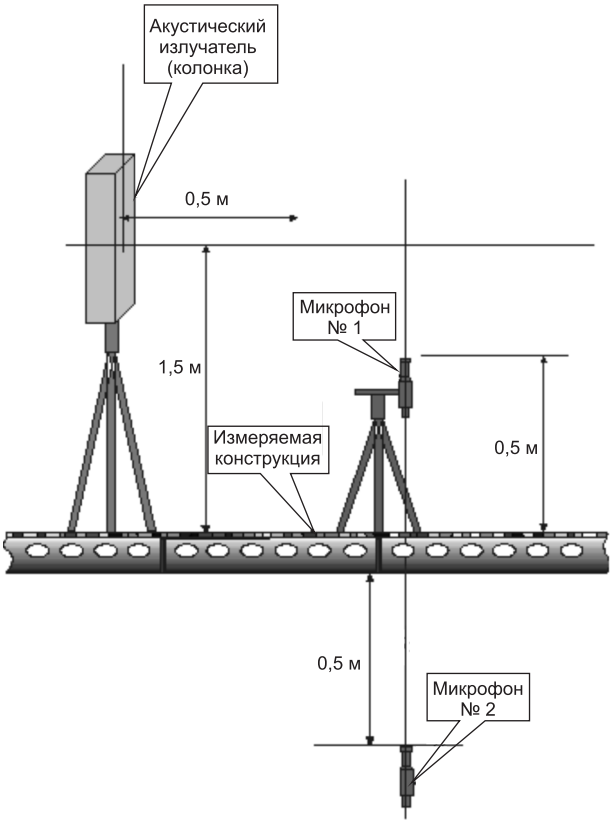


Схема 2. Расстановка микрофонов при измерениях перекрытий пола

Во время измерений перекрытия потолка микрофон № 1 размещался на расстоянии 0,5 м от него и развёрнут вертикально вниз. Микрофон № 2 — над перекрытием потолка в вышерасположенном помещении также на высоте 0,5 м и ориентирован по нормали к плоскости исследуемой конструкции.

При измерениях в системе вентиляции акустический излучатель размещался на высоте 1,5 м от уровня пола и направлен в сторону вентканала. Первый микрофон системы «Шепот» располагался на расстоянии 0,5 м от плоскости вентканала. Второй микрофон размещался на уровне вентканала на расстоянии 0,5 м от него (фото 3).

Ближайшими местами непреднамеренного прослушивания по акустическому каналу через окна ВП, являются соседние помещения № XX и № XX. Во время измерений окна ВП были закрыты, второй микрофон располагался на подоконнике ближнего к ВП окна, при этом створка окна была открытой (фото 6, 7).

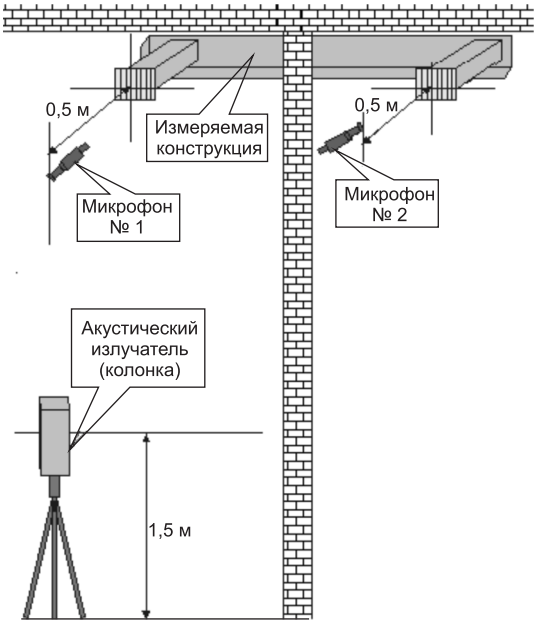


Схема 3. Расстановка микрофонов при измерениях системы вентиляции

Фото 6. Расположение первого микрофона

Фото 7. Расположение второго микрофона

7.3.2. Измерения на трубах системы отопления

В связи с тем, что граница КЗ проходит в точке выхода основных трубопроводов из здания, прямой замер защищённости невозможен. Обусловлено это тем, что на пути от ВП до точки измерения на границе КЗ вносится значительное затухание вибрационного тест-сигнала.

Исходя из изложенного, измерения системы отопления проводились методом реального затухания.

Система отопления подвергалась акустическому воздействию колонки. Наведенный на систему отопления сигнал измерялся во всех октавных полосах в двух точках — в непосредственной близости от излучателя тестового сигнала (10...15 см) и на границе КЗ (не ближе XX см до выхода за КЗ). Разность между значениями измеренных сигналов в двух точках и есть реальное затухание в исследуемой конструкции (схема 5). За реальное затухание, для упрощения расчетов, принималось минимальное из всех измеренных в октавных полосах.

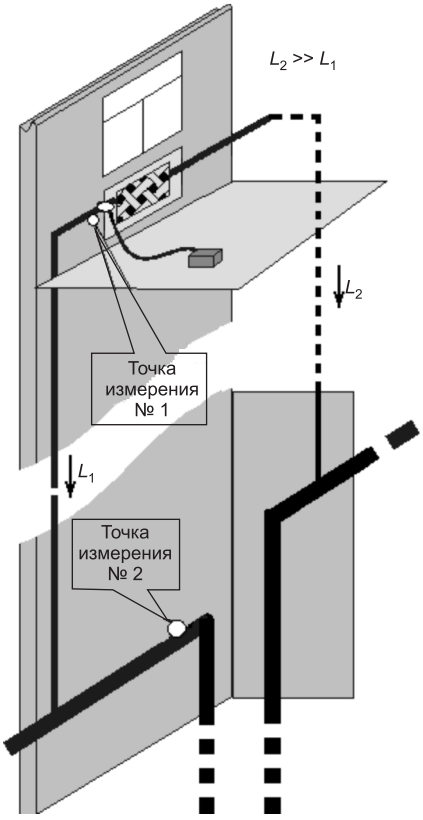


Схема 4. Измерение реального затухания в системе отопления

Следующим шагом проводилось измерение сигнала в системе отопления согласно схеме 5.

На результаты исследований, проведенных согласно схеме 5, накладывались результаты реально измеренного затухания в системе отопления.

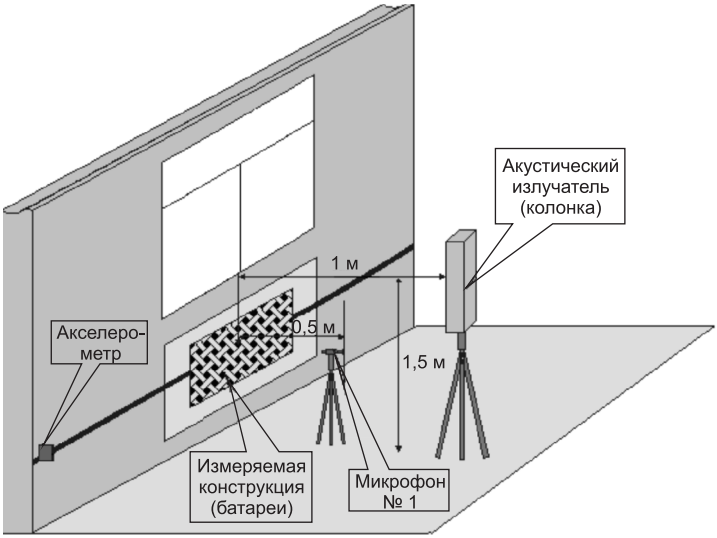


Схема 5. Измерение сигнала в системе отопления в ВП

По результатам анализа построения системы отопления на объекте, установлено, что минимальный пробег по трубе подачи горячей воды из городского ЦТП в ВП составляет 28,8 м (для ВП № XX) и минимальный пробег по трубе «обратки» составляет 33,1 м (для ВП № XX). Измерения реального затухания проводились на кратчайших расстояниях от ВП до выхода трубы из здания объекта. При проведении реального затухания первая точка бралась в месте, где располагался акселерометр при замере по схеме 6, вторая точка в техническом помещении на трубах подачи и «обратки».

В связи с тем, что во время проведения измерений была запущена в эксплуатацию система отопления (отопительный сезон), фоновые значения шумов при измерениях составляли порядка 40 дБ. Для ужесточения требований к полученным результатам фоновые шумы искусственно были занижены и приняты равными фоновым шумам на аналогичных чугунных радиаторах отопления на других объектах, но в летнее время года (в отсутствии шумов насосов и воды).

При измерениях в техническом помещении в некоторых октавных полосах, в связи с высокими уровнями фоновых значений, не удалось обнаружить сигнал от воздействующей на систему отопления акустической колонки. В этом случае за опасный сигнал принимались значения фоновых помех, измеренные в техническом помещении.

В результате измерений по кратчайшим расстояниям от ВП № и ВП№ (подача и «обратка») минимальное затухание распространения опасного сигнала во всех октавных полосах составило:

- для трубы подачи воды — 48,5 дБ;
- для трубы «обратки» — 52,7 дБ.

Для упрощения расчётов при оценке защищённости системы отопления и создания «запаса» по защищённости выбран минимальный из всех измеренных коэффициент затухания равный 48 дБ.

8. Таблицы результатов измерений и расчётов показателя противодействия

Таблицы измерений и расчетов приведены в Приложении 1, которое является неотъемлемой частью Протокола.

Далее, на рассмотрение представлена сводная таблица результатов измерений. В сводной таблице приведены КТ с максимальными значениями словесной разборчивости по каждому из направлений.

Таблица 2

Исследуемая конструкция	Применение системы виброакустического зашумления (да/нет)	Максимально полученное значение (W)
Вибрационный канал		
Система отопления	нет	0, 003
Акустический канал		
Дверной блок	да	0,07
Правая перегородка	нет	0,1
Левая перегородка	нет	0,08
Система приточной вентиляции	да	0,009
Перекрытие пола	нет	0,03
Перекрытия потолка в направлении чердака	нет	0,02
Окна в направлении соседних помещений	нет	0,06

9. Вывод

На основании проведенных исследований по виброакустической защищенности установлено, что для всех ограждающих конструкций и инженерно-технических систем помещения № X с учетом требований изложенных в «Частном техническом задании на выполнение работ...» (мк.XXXX) и «Программы проведения исследований...» (мк.XXXX), при штатно работающей системе активной защиты, нормы противодействия акустической речевой разведке **выполняются.**

Дата проведения контроля: с XX по XX февраля 201_года.
Контроль выполнили:
Руководитель группы инженеров X. Xxxxxxxx
Инженер X. Xxxxxxxxx
Дата проведения контроля: XX.XX.XX

Приложение № 4

Таблицы результатов измерений

Контрольная точка: КТ1.

Таблица 1

Параметр	Частота, Гц				
	250	500	1000	2000	4000
Уровень тест-сигнала	85,500	88,600	89,100	88,700	88,200
Уровень фона	36,000	32,800	31,800	31,100	29,400
Уровень сигнала	64,700	73,100	72,100	72,600	69,900
Уровень САЗ	64,800	60,600	61,100	56,600	56,500
Выполнение С/Ш	Да	Да	Да	Да	Да

В связи с тем, что во всех октавных полосах **достигнуто** требуемое соотношение сигнал/шум, труба системы отопления **защищена** от утечки по вибрационному каналу в данной контрольной точке.

Контрольная точка : КТ5. Дверной блок.

Таблица 2

Параметр	Частота, Гц				
	250	500	1000	2000	4000
Уровень тест-сигнала	85,700	88,900	89,100	88,600	88,200
Уровень фона	33,300	31,700	32,000	30,000	29,300
Уровень сигнала	56,700	70,100	73,500	69,100	69,500
Уровень САЗ	61,700	65,800	60,300	57,900	53,200
Выполнение С/Ш	Да	Да	Да	Да	Да

В связи с тем, что во всех октавных полосах **достигнуто** требуемое соотношение сигнал/шум, дверной блок **защищён** от утечки по акустическому каналу в данной контрольной точке.

Контрольная точка КТ 9. Правая перегородка. Канал вибрационный

Таблица 3

Параметр	Частота, Гц				
	250	500	1000	2000	4000
Уровень тест-сигнала	89,200	90,500	91,100	93,200	94,800
Уровень фона	32,100	27,500	28,800	30,300	29,000
Уровень сигнала	77,300	76,100	73,600	74,700	70,300
Уровень САЗ	51,800	59,500	55,300	56,700	54,600
Выполнение С/Ш	Нет	Нет	Нет	Да	Да
L_{CI}	77,2999	76,0999	73,5999	74,6998	70,2997
V_{LT}	23,2000	24,5000	30,1000	37,2000	41,8000
E	2,2999	−7,9001	−11,8001	−19,2002	−26,1003
z	0	0	0	0	0
	0,0030	0,0043	0,0088	0,0055	0,0012

R = 0,022862
Интегральная оценка (W) = 0,133152

В связи с тем, что в октавных полосах 250–1000 Гц **не достигнуто** требуемое соотношение сигнал/шум, вычисляется значение словесной разборчивости. $W < \delta_{\text{н}}$, перегородка **защищена** от утечки по вибрационному каналу в данной контрольной точке.

Контрольная точка КТ11. Левая перегородка. Канал вибрационный

Таблица 4

Параметр	Частота, Гц				
	250	500	1000	2000	4000
Уровень тест-сигнала	87,000	90,900	91,000	92,700	93,500
Уровень фона	42,000	39,000	37,000	33,000	30,000
Уровень сигнала	57,100	55,200	51,100	58,400	60,600
Уровень САЗ	46,900	50,600	42,500	40,200	35,700
Выполнение С/Ш	Да	Да	Да	Да	Нет
L_{CI}	56,9637	55,0946	50,9277	58,3875	60,5962
V_{LT}	21,0000	24,9000	30,0000	36,7000	40,5000
E	−10,9363	−20,4054	−21,5723	−18,5125	−15,6038
z	0	0	0	0	0
r	0,0002	0,0002	0,0010	0,0064	0,0118
R = 0,019770					
Интегральная оценка (W) = 0,112864					

В связи с тем, что в октавной полосе 4000 Гц **не достигнуто** требуемое соотношение сигнал/шум, вычисляется значение словесной разборчивости. W< $\delta_{\text{н}}$ перегородка **защищена** от утечки по вибрационному каналу в данной контрольной точке.

Контрольная точка КТ16. Система вентиляции.

Таблица 5

Параметр	Частота, Гц				
	250	500	1000	2000	4000
Уровень тест-сигнала	74,600	79,800	81,900	82,900	81,600
Уровень фона	35,600	31,300	29,000	30,400	30,000
Уровень сигнала	71,100	68,300	61,200	56,400	50,400
Уровень САЗ	73,600	67,900	56,700	49,900	45,900
Выполнение С/Ш	Да	Да	Да	Да	Да

В связи с тем, что во всех октавных полосах **достигнуто** требуемое соотношение сигнал/шум, вентиляция **защищена** от утечки по акустическому каналу.

Приложение № 5

Вариант плана проведения комплексной специальной проверки помещений

Конфиденциально
Экз. №_
Всего экз. __

Согласовано
Начальник службы безопасности
« »_____ 201___ г.

Утверждаю
Руководитель предприятия
« »_____ 201___ г.

План
проведения комплексной специальной проверки помещений

1. Выводы из оценки противника

В качестве субъекта, выбранного вероятным противником для внедрения средств НСИ, рассматривается посетитель (клиент), имевший доступ в кабинет руководителя предприятия и в соседние с ним помещения. Для внедрения средств НСИ возможно использование противником одного из строительных рабочих, проводивших косметический ремонт кабинета руководителя в период с _____ по _____ (дата, время). В качестве субъекта, осуществляющего съём информации, рассматривается посетитель (клиент) или посторонние лица за пределами контролируемой зоны.

Субъект, осуществлявший внедрение средств НСИ, является специалистом по негласному съёму информации, обладает сведениями о расположении интересующих его помещений, размещении в них оборудования и предметов интерьера.

Учитывая возможность установки средств НСИ во время ремонта кабинета руководителя, можно ожидать использования противником как радиоизлучающих средств НСИ, так и передающих информацию по проводам. В соседних помещениях возможна установка противником средств съёма информации с телефонных линий и электронных стетоскопов. Ожидаемый технический и технологический уровень применяемых средств НСИ соответствует среднему участку ценового диапазона этих средств.

Наиболее вероятна установка средств НСИ во время ремонта кабинета руководителя путём подброса, подключения к телефонной линии, подмены электроустановочных и телефонных коммутационных изделий. Возможен подброс радиомикрофона во время посещения кабинета посетителем (клиентом).

Вероятное время установки (внедрения) средств НСИ — в период с_____ по _____ (дата, время). Ожидаемые способы съёма информации — подключение к проводным линиям в соседних помещениях и перехват радиопередач с помощью радиоконтрольного пункта, размещённого за пределами охраняемой территории.

При обнаружении противником намерений провести специальную проверку помещений возможно временное изъятие средств НСИ. Установление факта проведениятакой проверки может привести к временному отключению дистанционно управляемых средств НСИ. При установлении факта обнаружения внедрённых средств НСИ наиболее вероятна попытка внедрения нового аналогичного устройства.

2. Замысел проведения комплексной специальной проверки помещений

Цель проведения проверки — предотвращение ущерба от утечки информации из помещения через возможно внедрённые средства НСИ.

Проверке подлежат:

1. Кабинет руководителя предприятия.

Площадь помещения ___ кв. м., объём ___ куб. м. Ограждающие конструкции — железобетонные панели (толщина наружной стеновой панели ___ см, двух внутренних стеновых панелей ___ см, пола и потолочного перекрытия ___ см), смежная с бухгалтерией стена — кирпичная, толщиной ___ см. Потолок подвесной, стены оштукатуренные, отделанные деревянными панелями. Два вентиляционных канала естественной вентиляции.

Телевизор, ПЭВМ, телефонный аппарат. Мебель стандартная офисная: письменный и журнальный столы, стол для посетителей, шесть стульев, встроенный шкаф, два стеллажа, два мягких кресла, диван, сейф, холодильник занимают ___ % общей площади помещения.

Проводные коммуникации силовой и осветительной сети, телефонная линия, линии пожарной и охранной сигнализации. Магистраль парового отопления.

2. Комната для проведения переговоров.

(приводятся характеристики второго помещения)

Перечень запланированных работ:

1. В кабинете руководителя предприятия:

1. Визуальный осмотр ограждающих конструкций, мебели и других предметов интерьера (ожидаемая трудоёмкость ___ чел/часов).

2. Проверка элементов строительных конструкций, мебели и других предметов интерьера с использованием специальных поисковых технических средств (___ чел/часов).

3. Проверка линий и оборудования силовой и осветительной электросети (___ чел/часов).

4. Проверка линий и оборудования абонентской телефонной сети (___ чел/часов).

5. Проверка линий и оборудования пожарной и охранной сигнализации (___ чел/часов).

6. Проверка радиоэфира на присутствие сигналов радиоизлучающих средств негласного съёма информации (радиомониторинг помещения) (___ чел/часов).

7. Проверка несанкционированных передач информации в диапазоне инфракрасного излучения (___ чел/часов).

8. Поиск средств негласного съёма и передачи информации, внедрённых в электронные приборы (___ чел/часов).

2. На внешней, выходящей на улицу поверхности стены кабинета руководителя:

Визуальный осмотр ограждающих конструкций (___ чел/часов).

3. В помещении секретаря (смежном с кабинетом руководителя):

(приводится перечень запланированных работ)

4. В комнате для проведения переговоров:

(описываются проверяемые помещения и перечень запланированных в них работ)

Время проведения специальной проверки:

с _____ до _____ (дата, время). Общая продолжительность непосредственного проведения проверки ___ часов.

Легенда прикрытия предварительного осмотра помещений:

Осмотр помещений для составления сметы на текущий ремонт помещений (с ___ до ___ (дата, время)). Доводится под запись до секретаря и ответственного за эксплуатацию здания за три дня до осмотра (дата).

Документ подтверждающий легенду — копия договора на выполнение работ.

Легенды прикрытия поисковых работ:

1. Проверка специалистами телефонного узла связи состояния телефонных линий и оборудования (с ___ до ___ (дата, время)). Доводится под запись до секретаря за два дня до проверки (___ дата).

Документы, подтверждающие легенду — наряд на проведение работ и допуск для работ на оборудовании.

2. Поиск местонахождения искрящих контактов скрытой электропроводки для устранения помех ПЭВМ (с _____ до _____ (дата, время)). Доводится до секретаря и ответственного за электрохозяйство накануне проверки (_____ дата).

Документ подтверждающий легенду — копия договора на выполнение поисковых работ.

Меры по активации внедренных средств съёма информации:

Доведение до секретаря и лиц руководящего состава предприятия информации о проведении в день проверки совещания руководящего состава предприятия по вопросам ускорения разработки новых образцов продукции и продвижения их на рынок товаров и услуг. Способ доведения — распространение среди лиц руководящего состава повестки дня совещания и распоряжения о подготовки докладов.

Дата доведения: ___ (за неделю до начала проверки).

Действия в случае обнаружения средств негласного съёма информации:

Не трогая обнаруженное средство, доложить о факте обнаружения руководителю и начальнику службы безопасности предприятия для принятия решения о дальнейших действиях.

3. Привлекаемые силы и средства, их распределение по объектам и видам работ

Состав поисковой бригады:

1. Руководитель.
2. _____
3. _____

Перечень специального, оборудования и технических средств, привлекаемых для проведения проверки:

1. Комплект досмотровых зеркал «XXXXXX» (применяется только при закрытых дверях помещения и отсутствиив нём посторонних лиц).

2. Прибор нелинейной радиолокации «XXXXXX» (в процессе радиомониторинга не включать, применять только при закрытых дверях помещения и отсутствии в нём посторонних лиц).

3. _____

(далее продолжается перечень оборудования и технических средств с указанием основных особенностей их применения в рамках выбранных легенд прикрытия и других ограничений, налагаемых условиями проверки)

Распределение специалистов поисковой бригады, оборудования и технических средств по видам работ и объектам специальной проверки:

Оформляется в виде таблицы или сетевого графика с описанием перечня работ порядка выполнения (последовательного или параллельного), применяемого при этом оборудования.

Дополнительные меры по активизации внедренных средств НСИ:

В кабинете руководителя для активизации средств НСИ с акустопуском с помощью магнитолы воспроизводится предварительно сделанные на научной конференции записи докладов. В комнате для пе-

реговоров воспроизводятся предварительно сделанные записи обсуждения «конфиденциальных» деловых вопросов. Начало воспроизведения записей — с началом проведения визуального осмотра ограждающих конструкций, мебели и других предметов интерьера помещений.

При проверке наличия сигналов в проводных линиях всё подключённое к ним оборудование приводится в рабочее состояние (включается в рабочий режим), трубки телефонных аппаратов снимаются для перевода телефонных линий в режим «занято».

4. Перечень подготавливаемых по результатам проверки итоговых и отчётных документов и срок их представления для утверждения

1. Акт проведения комплексной специальной проверки помещений.
2. Описание проведённых работ и исследований.
3. Рекомендации по повышению надёжности защиты информации от её возможной утечки по техническим каналам.
4. Журнал регистрации заводских и инвентарных номеров оборудования, мебели и предметов.
5. Журнал регистрации пломб и скрытых меток.

Акт проведения проверки помещений — в двух экземплярах (один — исполнителям работ). Остальные документы в единственном экземпляре.

Все документы с грифом «коммерческая тайна». Срок представления для утверждения _____.

Согласовано

Руководитель организации проводящей проверку

_____

Руководитель поисковой бригады

_____

Члены поисковой бригады

_____

« » _____ 201___ г.

Приложение № 6

Вариант акта проведения комплексной специальной проверки помещений

Коммерческая тайна
Экз. № ___
Всего экз. ___

Согласовано
Руководитель организации проводившей проверку

_____
« » _____ 201___ г.

Утверждаю
Руководитель предприятия

_____

Акт
проведения комплексной специальной проверки помещений

1. В период с ___ по ___ на предприятии (наименование предприятия) проведена комплексная специальная проверка помещений.
2. Состав поисковой бригады:
    1. Руководитель _____
    2. _____
    3. _____
3. Проверены следующие помещения:
    1. Кабинет руководителя предприятия.
    2. Комната для переговоров.
    3. _____
4. В ходе проверки проведены следующие работы:

4.1. Визуальный осмотр ограждающих конструкций, мебели и других предметов интерьера (трудозатраты — ___ чел/часов).

4.2. Проверка элементов строительных конструкций, мебели и других предметов интерьера с использованием специальных поисковых технических средств (___ чел/часов).

4.3. Проверка линий и оборудования силовой и осветительной электросети (___ чел/часов).

4.4. Проверка линий и оборудования абонентской телефонной сети (___ чел/часов).

4.5. Проверка линий и оборудования пожарной и охранной сигнализации (___ чел./часов).

4.6. Проверка радиоэфира на присутствие сигналов радиоизлучающих средств негласного съёма информации (радиомониторинг помещения) (___ чел./часов).

4.7. Проверка несанкционированных передач информации в диапазоне инфракрасного излучения (___ чел/часов).

4.8. Поиск средств негласного сьёма и передачи информации, внедрённых в электронные приборы (_____чел/часов).

4.9. Визуальный осмотр внешних, выходящих на улицу поверхностей стен кабинета руководителя и помещения бухгалтерии (___ чел/часов).

4.10. Визуальный осмотр и проверка элементов строительных конструкций, проводных и технологических коммуникаций в соседних с проверяемыми помещениях (___ чел/часов).

5. В ходе проверки использовалась следующая поисковая и исследовательская аппаратура:

5.1. Комплект досмотровых зеркал XXXXXXX (№___).

5.2. Комплект луп, фонарей.

5.3. Гибкий технический эндоскоп с дистальным концом XXXXX XX (зав. №___).

5.4. Досмотровый селективный металлоискатель XXXXX (зав. №___).

5.5. Прибор нелинейной радиолокации XXXXX (зав. №___).

5.6. Переносный флуороскоп ФП-1 (зав. №___).

5.7. Многофункциональный поисковый прибор XXX (зав. №___).

5.8. Комплекс обнаружения радиоизлучающих средств и радиомониторинга XXXXXXX (зав. №___).

5.9. Обнаружитель скрытых видеокамер XXXX (зав. №___).

5.10. Дозиметр поисковый (прибор радиационного контроля) XXXXXXXX (зав. №___).

6. Результаты проверки

6.1. В кабинете руководителя обнаружено подслушивающее устройство с передачей перехватываемой акустической информации по проводам силовой электрической сети. Устройство на момент проверки работоспособно, выполнено в виде тройника-разветвителя и подключено к розетке электрической сети возле рабочего стола руководителя предприятия. Радиус съёма акустической информации около 6 метров, дальность передачи перехватываемой информации — до силового трансформатора, размещённого в электросиловой будке, находящейся за пределами охраняемой территории.

Обнаруженное подслушивающее устройство нейтрализовано акустической изоляцией микрофона и оставлено на месте обнаружения.

Других средств негласного съёма информации в кабинете руководителя не обнаружено.

6.2. В помещении бухгалтерии средств негласного съёма информации не обнаружено.

6.3. Кабинет руководителя предприятия недостаточно защищен от утечки защищаемой информации по техническим каналам:

- возможна утечка акустической информации через канал естественной вентиляции помещения;
- возможна утечка акустической информации через виброакустический канал, образованный магистралью парового отопления;
- возможен несанкционированный съём информации с монитора компьютера при перехвате его ПЭМИ.

6.4. Комната для переговоров не защищена от утечки защищаемой информации по техническим каналам:

- возможна утечка акустической информации через тонкую дверь и гипсокартонную часть перегородки с помещением приёмной;
- возможна утечка акустической информации через канал естественной вентиляции помещения;
- возможна утечка акустической информации через виброакустический канал, образованный магистралью парового отопления;
- существует возможность дистанционного, без подключения дополнительных устройств перехвата телефонных переговоров, ведущихся с радиотелефона PANASONIC;
- возможен несанкционированный съём информации с мониторов компьютеров и другой оргтехники путём перехвата ПЭМИ;
- возможна утечка информации, снимаемой визуально или с использованием фото- и видеотехники, через не зашторенное окно и застеклённую часть входной двери.

6.5. Оба помещения не защищены от несанкционированной записи конфиденциальных переговоров на диктофон, съёмки скрытыми видеокамерами и возможной утечки информации за счёт наводок в проводных линиях, проложенных параллельно проводам телефонной сети. Помещения имеют много мест, удобных для подброса радиомикрофонов или быстрой установки других видов средств негласного съёма информации.

7. Рекомендации по повышению защищённости проверенных помещений и предотвращения утечки информации по выявленным техническим каналам её утечки изложены в отдельном документе.

Приложение № 7

Рекомендации по повышению защищённости помещений и объектов (вариант)

Коммерческая тайна
Экз. № ___
Всего экз. ___

Рекомендации по повышению защищённости помещений

I. Перечень выявленных в проверенных помещениях потенциальных технических каналов утечки информации (ТКУИ)

А. Кабинет руководителя предприятия:

1) акустический воздушный ТКУИ через канал естественной вентиляции помещения;

2) акустический вибрационный ТКУИ через канал естественной вентиляции помещения;

3) акустический вибрационный ТКУИ через магистраль (трубопровод) парового отопления помещения;

4) электромагнитный ТКУИ за счёт перехвата ПЭМИ монитора компьютера;

5) электрические ТКУИ за счёт съёма наводок с проводных линий пожарной и охранной сигнализации, проложенных параллельно проводам телефонной линии.

Б. Помещение бухгалтерии:

1) акустический воздушный ТКУИ через канал естественной вентиляции помещения;

2) акустический воздушный ТКУИ через входную дверь помещения;

3) акустический воздушный ТКУИ через гипсокартонную перегородку с помещением приёмной;

4) акустический вибрационный ТКУИ через канал естественной вентиляции помещения;

5) акустический вибрационный ТКУИ через гипсокартонную перегородку с помещением приёмной;

6) акустический вибрационный ТКУИ через магистраль (трубопровод) парового отопления помещения;

7) электромагнитные ТКУИ за счёт перехвата ПЭМИ мониторов компьютеров и другой оргтехники;

8) электрические ТКУИ за счёт съёма наводок с проводных линий пожарной и охранной сигнализации, проложенных параллельно проводам телефонной линии;

9) возможна утечка информации за счёт прямого перехвата сигналов радиотелефона Panasonic;

10) возможна утечка информации, снимаемой визуально или с использованием фото- и видеотехники, через незашторенное окно и застеклённую часть входной двери.

Оба помещения не защищены от несанкционированной записи на диктофон, съёмки скрытыми видеокамерами и подброса радиомикрофонов. Схемы выявленных потенциальных ТКУИ с краткими пояснениями (легендами) — в приложении № 1 к документу.

II. Оценка вероятности использования противником потенциальных ТКУИ и защищённости помещений

А. Кабинет руководителя предприятия:

1. Ввиду хорошей слышимости и разборчивости речевых сигналов и доступности для противника соседних помещений вероятности использования противником акустического воздушного и акустического вибрациионного потенциальных ТКУИ можно считать *высокими*.

2. Использование противником акустического вибрационного ТКУИ через магистраль (трубопровод) парового отопления из-за слабой разборчивости сигналов можно считать *вероятным*.

3. Использование противником электромагнитного ТКУИ за счёт перехвата ПЭМИ монитора компьютера и электрического ТКУИ за счёт съёма наводок с проводных линий можно считать *маловероятным*, но возможным. В связи с отсутствием в кабинете специальных средств защиты информации от её утечки по выявленным потенциальным ТКУИ и высокой вероятностью использования противником акустического воздушного и акустического вибрационного потенциальных ТКУИ кабинет руководителя предприятия следует считать *незащищённым* от утечки защищаемой информации по техническим каналам.

Б. Помещение бухгалтерии:

(далее даётся оценка вероятности использования противником потенциальных ТКУИ и оценка защищённости помещения от негласного съёма информации)

III. Рекомендации по мерам и способам предотвращения съёма информации по выявленным потенциальным ТКУИ и повышению защищённости помещений

А. Кабинет руководителя предприятия:

1. Для защиты помещения от утечки акустической информации через канал естественной вентиляции помещения рекомендуется зашумление канала за счет создания акустических и вибрационных по-

мех с помощью генератора акустического шума. Наиболее эффективной системой защиты является комплекс виброакустической защиты XXXXXXX. Частичной, более дешёвой альтернативой комплексу можно считать генератор акустического шума XXXXX.

Эти же средства обеспечат защиту помещения от утечки акустической информации через магистраль (трубопровод) парового отопления и ограждающие кабинет строительные конструкции.

2. Для защиты помещения от утечки информации за счёт перехвата ПЭМИ монитора компьютера рекомендуется электромагнитное зашумление помещения с помощью генератора шума XXXXX. Применение этого генератора обеспечит также создание помех средствам несанкционированного съёма информации с электрической сети, что предотвратит утечку информации в случае повторного использования противником подслушивающего устройства, аналогичного найденному в ходе проверки. В качестве альтернативы генератору шума XXXXXX по электромагнитному зашумлению помещения может рассматриваться генератор шума XXXX или XXXXXXX.

3. Для предотвращения утечки информации за счёт съёма наводок спроводных линий пожарной и охранной сигнализации рекомендуется перепрокладка телефонной линии для устранения её совместного параллельного пробега с линиями пожарной и охранной сигнализации. Альтернативой перепрокладки телефонной линии является установка в линиях пожарной и охранной сигнализации помехоподавляющих фильтров XXXXX.

4. Для защиты помещения от несанкционированной аудиозаписирекомендуется применение подавителя радиоэлектронных устройств негласной аудиозаписи XXXXXXX.

5. Для своевременного обнаружения несанкционированной видеосъёмки рекомендуется усилить режимные меры по посещению и регулярная проверка кабинета с использованием обнаружителя скрытых видеокамер XXXXXXX.

Б. Помещение бухгалтерии:

1. Для защиты помещения от утечки акустической информации... (далее даются рекомендации по мерам и способам предотвращения съёма информации по выявленным ТКУИ и повышению защищённости помещения бухгалтерии)

IV. Сводный перечень технических средств и систем защиты информации, рекомендуемых для повышения защищённости помещений

Таблица 1

№ п/п	Рекомендуемое средство	Альтернативное средство	Назначение	Кол-во
		Кабинет руководителя предприятия		
1	Комплекс виброакустической защиты XXXXX	Генератор акустического шума XXXXXX	Защита помещения от утечки акустической информации через канал естественной вентиляции, трубопровод отопления, ограждающие строительные конструкции	1
2	Генератор шума XXXXXX	Генератор шума XXX или XXX (защиту электрической сети не обеспечивают)	Защита помещения от утечки информации за счёт перехвата ПЭМИ компьютера и съёма информации с электрической сети	1
3	Помехоподавляющий фильтр XXXX		Предотвращение утечки информации за счёт съёма наводок с проводных линий пожарной и охранной сигнализации	2
4	Подавитель радиоэлектронных устройств негласной аудиозаписи XXXXXXX		Защита помещения от несанкционированной записи на диктофон	1
5	Обнаружитель скрытых видеокамер XXXXX	Нет аналогов	Своевременное обнаружение несанкционированной видеосъемки в помещении	1
		Помещение бухгалтерии		
6 7 8 9 10 11	Далее продолжается перечень технических средств и систем защиты информации, рекомендуемых для повышения защищённости помещения бухгалтерии			
		Помещение службы безопасности		
12	Комплекс обнаружения радиоизлучающнх средств радиомониторинга XXXXXXX	Многофункциональный комплекс радиоконтроля XXXXXXX	Оборудование пункта радиоконтроля для постоянного (круглосуточного) радиомониторинга служебных помещений	1
13 14	Многоканальный цифровой магнитофон XXXXXX		Обеспечение гласного санкционированного контроля акустики служебных помещений и установленных руководством ограничений на использование телефонных каналов связи	1

V. Предложения по практическому использованию рекомендуемых средств и систем защиты информации

1. Комплекс виброакустической защиты XXXX способен обеспечить одновременную защиту всех проверенных помещений.

В кабинете руководителя предприятия целесообразно установить одно устройство контроля эффективности вибрационных помех XXXX шесть виброгенераторов типа XXXXXXX: по одному в каждом вентиляционном канале, по одному на стекло окна, на трубопровод парового отопления, балку потолочного перекрытия и на плиту перекрытия между вторым и третьим этажами.

В помещении бухгалтерии целесообразно установить четыре виброгенератора типа XXXXXXX и одно устройство контроля эффективности вибрационных помех XXXXXXX. Рекомендуемые места установки отражены на схеме приложения №2.

Установку основного блока (генератора) комплекса виброакустической защиты устройства дистанционного включения виброгенераторов XXXXXXXX рекомендуется провести в помещении службы безопасности.

Включение помехового сигнала в защищаемых помещениях рекомендуется осуществлять из помещения службы безопасности на время ведения конфиденциальных переговоров. Контроль эффективности помех целесообразно осуществлять по сигналу тревоги, подаваемому устройствами XXXXXXXX, установленными в защищаемых помещениях.

2. Генераторы шума XXXXXXXX рекомендуется установить по одному в каждом защищаемом помещении.

Включение электромагнитного зашумления помещения в кабинете руководителя предприятия целесообразно осуществлять на время работы с ПЭВМ, в помещении бухгалтерии — с началом рабочего дня.

Включение режима линейного зашумления электросети рекомендуется с началом рабочего дня, выключение — по его окончании.

Режим защиты телефонной линии генератора шума XXXXXX в кабинете руководителя предприятия использовать не рекомендуется в связи с применением для этой цели более эффективного устройства защиты XXXXXXXXX.

3. Установку помехоподавляюших фильтров XXXXX в линии пожарной и охранной сигнализации защищаемых помещений рекомендуется осуществить согласно схемам приложения № 2.

4. Подавитель радиоэлектронных устройств негласной аудиозаписи XXXXXX рекомендуется включать с помощью пульта дистанционного управления на время проведения совещаний и конфиденциальных переговоров.

(далее продолжаются предложения по практическому использованию средств и систем защиты информации, рекомендованных для повышения защищённости помещений)

Приложения (не прилагаются)

1. Схемы выявленных по результатам проверки потенциальных технических каналов утечки информации.
2. Схемы установки рекомендуемых средств и систем защиты информации.

Согласовано

Руководитель организации проводящей проверку

_____

Руководитель поисковой бригады

_____

Члены поисковой бригады

_____

« » _____ 201___ г.

Литература

1. **Абалмазов Э.И.** Направленные микрофоны. Мифы и реальность // Системы безопасности связи и телекоммуникаций. 1996. № 4. С. 98–101.

2. **Абалмазов Э.И.** Новые технологии защиты телефонных переговоров // Специальная техника. 1998. № 1. С. 4–8.

3. **Акустика.** Справочник: Под общ. ред. М.А. Сапожкова. — М.: Радио и связь, 1989. — 336 с.

4. **Алексеенко В.Н., Петраков А.В., Лагутин В.С**. Техническая защита информации // Вестник связи. 1994. № 12. С. 27–34; 1995. № 2. С. 26–29; № 3. С. 29–30; № 5. С. 23–28.

5. **Андрианов В.И., Бородин В.А., Соколов А.В.** «Шпионские штучки» и устройства для защиты объектов и информации: Справочное пособие. — С-Пб: Лань, 1996. — 272 с.

6. **Анисимов Ю.** «Ольха» — новое решение для систем цифровой записи и компьютерной телефонии // Системы безопасности связи и телекоммуникаций. 1999. № 24. С. 94–95.

7. **Аттестат** соответствия прилагается // Защита информации. «Конфидент». 1999. Май-июнь. С. 79–83.

8. **Балахничев И.М., Дрик А.В., Крупа А.И.** Борьба с телефонным пиратством. — Минск: ОМО «Наш город», 1998. — 127 с.

9. **Барсуков В.С.** Безопасность: технологии, средства, услуги. — М.: КУДИЦ-ОБРАЗ, 2001. — 496 с.

10. **Барсуков В.С., Марущенко В.В., Шичин В.А.** Интегральная безопасность. - – М.: РАО «Газпром», 1990. — 170 с.

11. **Бейли Д., Райт Э.** Волоконная оптика: теория и практика. Пер. с англ. М.: КУДИЦ-ПРЕСС, 2010. — 320 с.

12. **Бенин М.С., Подунов А.С.** Звукотехника. — М.: ДОСААФ СССР, 1976. — 159 с.

13. **Брусницын Н.Л.** Открытость и шпионаж. — М.: Воениздат, 1991. — 56 с.

14. **Болдырев А.И., Василевский И.В., Сталенков С.Е.** Методические рекомендации по поиску и нейтрализации средств негласного съёма информации. — М. ЗАО НПЦ Фирма «НЕЛК», 2001. — 138 с.

15. **Бузов Г.А., Калинин С.В., Кондратьев А.В.** Защита от утечки информации по техническим каналам: Учеб. пособие. — М.: Горячая линия — Телеком, 2005. — 416 с.

16. **Бузов Г.А.** Практическое руководство по выявлению специальных технических средств несанкционированного получения информации: Учеб. пособие.— М.: Горячая линия — Телеком, 2010. — 240 с.

17. **Василевский И.В., Белорусов Д.И.** Методы и способы защиты телефонных линий // Специальная техника. 1999. № 5. С. 11–14.

18. **Василевский И.В., Белорусов Д.И.** Модульная архитектура компьютерной защиты речевой информации // Специальная техника. 1999. № 4. С. 24–28.

19. **Вернигоров Н.С.** Критическое замечание на «реальный взгляд» эксперта // Защита информации. «Конфидент». 1999. № 2. С. 53–54.

20. **Вернигоров Н.С.** Нелинейный локатор — эффективное средство обеспечения безопасности в области утечки информации. // Защита информации. «Конфидент». 1996. № 1. С. 67–70.

21. **Вернигоров Н.С.** Особенности устройств съема информации и методы их блокировки. — Томск: В-Спектр, 2006.

22. **Вернигоров Н.С.** Положите трубку, Вас подслушивают // Защита информации. «Мир безопасности». 1998. С. 109–119.

23. **Волобуев С.В.** Оценка акустической защищенности без применения инструментальных средств // Системы безопасности связи и телекоммуникаций. 1999. № 25. С. 38–45.

24. **Волгин М.Л.** Паразитные связи и наводки. — М.: Советское радио, 1965. — 232 с.

25. **Вус М.А.** Информация — ваш самый дорогой товар // БДИ. 1995. № 1. С. 21–23.

26. **Гавриш В.Ф.** Практическое пособие по защите коммерческой тайны. — Симферополь: Таврида, 1994. — 112 с.

27. **Герасименко В.А.** Защита информации в автоматизированных системах обработки данных. В 2 кн. — М.: Энергоатомиздат, 1994.

28. **Герасименко В.А., Малюк А.А.** Основы защиты информации. — М.: МИФИ, 1998. — 538 с.

29. **ГОСТ РВ 50170-92**. Противодействие ИТР. Термины и определения. — М.: Госстандарт России, 1992.

30. **ГОСТ 28147-89.** Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования. — М.: Госстандарт СССР, 1989.

31. **ГОСТ Р 50992-96**. Защита информации. Термины и определения. — М.: Госстандарт России.

32. **Гришачев В.В., Халяпин Д.Б., Шевченко Н.А., Мерзликин В.Г.** Новые кананы утечки конфиденциальной речевой информации

через волоконно-оптические подсистемы СКС // Специальная техника. 2009. № 2. С. 2–9.

33. **Гришачев В.В., Халяпин Д.Б., Шевченко Н.А.** Новые каналы утечки конфиденциальной речевой информации через волоконно-оптические подсистемы СКС. 2012 г., интернет ресурс. http://www.batman.ru/content/articles/index.php?article= 21627

34. **Девойно С.** Безопасность телефонных переговоров — проблема, имеющая решение // Защита информации. «Мир безопасности». 1998. С. 42–49.

35. **Ефимов А.И., Вихорев С.В.** Обеспечение информационной безопасности // Системы безопасности связи и телекоммуникаций. 1996. № 3. С. 82–83.

36. **Заборов В.И., Лалаев Э.М., Никольский В.К.** Звукоизоляция в жилых и общественных зданиях. — М.: Стройиздат, 1979. — 154 с.

37. **Защита** информации. Инсайд. Цикл статей по защите информации и по поиску закладочных устройств. — 2013. № 2–6; 2014. № 1–2.

38. **Закон РФ** «О государственной тайне» от 21 июля 1998. № 5486-1. Индукционный съем информации с телефонной линии — можно ли с ним бороться // Мы и безопасность. 1996. № 2. С. 10–11.

39. **Закон РФ** «Об информации, информационных технологиях и защите информации» от 27 июля 2006 года // Консультант+ . 2006.

40. **Интернет ресурс.** Сайт bnti.ru. Ресурс «Техника для спецслужб».

41. **Калинин С.В.** О некоторых новых тенденциях в развитии систем виброакустического зашумления // Защита информации. «Конфидент». 1999. № 4–5. С. 74–79.

42. **Каталог** специальных технических средств для проведения поисковых мероприятий и защиты от несанкционированного съема информации. — М.: «Юнитех», в/о Внештехника, 2000. — 25 с.

43. **Каталог** Центра безопасности информации «МАСКОМ». — М., 2003. — 52 с.

44. **Киселькov А.П. Кочетков Е.И.** Вас прослушивают // Защита информации. «Конфидент». 1999. № 3.

45. **Козюренко Ю.И**. Звукозапись с микрофона. — М.: Радио и связь, 1998. — 111 с.

46. **Кравчук П.Н.** Генерация и методы снижения шума и звуковой вибрации. — М.: Изд-во МГУ, 1991. — 183 с.

47. **Крысин А.В.** Безопасность предпринимательской деятельности. — М.: Финансы и статистика, 1996. — 379 с.

48. **Лунегов А.И., Рыжов А.Л.** Технические средства и способы добывания и защиты информации. — М.: ВНИИ «Стандарт», 1993. — 95 с.

49. **Лысов А.В.** Лазерные микрофоны — универсальные средства разведки или очередное поветрие моды // Защита информации. «Конфидент». 1997. № 1. С. 61–62.

50. **Лысов А.В., Остапенко А.Н.** Телефоны и безопасность (Проблемы защиты информации в телефонных сетях). — С-Пб.: Лаборатория ППШ, 1995. — 105 с.

51. **Максименко В.Н., Афанасьев В.В., Волков Н.В.** Защита информации в сетях сотовой подвижной связи. — М.: Горячая линия — Телеком, 2007. — 360 с.

52. **Маркоменко В.И.** Защита информации в информационно-телекоммуникационных системах органов государственной власти // Системы безопасности связи и телекоммуникаций. 1997. № 1. С. 72–76.

53. **Мироничев С.** Коммерческая разведка и контрразведка или промышленный шпионаж в России и методы и борьбы с ним. — М.: Дружок, 1995. — 223 с.

54. **Направленные** микрофоны // Мы и безопасность. 1996. № 3. С. 12–13.

55. **Новый** прибор контроля и защиты телефонной линии // Системы безопасности связи и телекоммуникаций. 1998. № 21. С. 18–19.

56. **От стихии** рекламы — к цивилизованному рынку / С.Е. Сталенков, И.В. Василевский, А.М. Рембовский, В.В. Филипповский // Защита информации. Конфидент. 1998. № 3.

57. **Палий А.М.** Радиоэлектронная борьба. — М.: Воениздат, 1989. — 350 с.

58. **Петраков А.В., Лагутин В.С.** Утечка и защита информации в телефонных каналах. — М.: Энергоатомиздат, 1997. — 298 с.

59. **Петров Н.Н.** «Скорпион» — новое отечественное изделие радиомониторинга // Специальная техника. 1998. № 2.

60. **Покровский Н.Б.** Расчет и измерение разборчивости речи. — М.: Связьиздат, 1962.

61. **Поляков А.В.** Промышленный шпионаж и как с ним бороться // Мы и безопасность. 1996. № 2. С. 22–24.

62. **Попугаев Ю.** Телефонные переговоры, средства защиты // Защита информации. Мир безопасности. 1998. С. 23–31.

63. **Прозрачные** переговорные кабины. История, настоящее, перспективы / Ю.П. Сафонов, А.Л. Белобородов, И.В. Савченко, В.П. Орлов // Защита информации. Конфидент. 1997. № 3. С. 57–61.

64. **Проспекты** фирм «Нелк», «Маском», «Энсанос», ИКМЦ, «Защита информации», «Мир безопасности», «Иркос», АОХК «Электрозавод» (Лаборатория № 11), «НОВО», «Сюртель» на выставках «Безопасность» 1996–2003.

65. **Пятачков А.Г.** О результатах исследования сетей электропитания технических средств, используемых для обработки конфиденциальной информации. Вопросы защиты информации. 1996. № 1. С. 26–30.

66. **Пятачков А.Г.** Рекомендации по защите информации от утечки по техническим каналам на объектах информатизации // Защита информации. «Конфидент». 1999. № 4–5. С. 80–85.

67. **Расторгуев С.П.** Абсолютная система защиты // Системы безопасности. 1996. Июнь-июль. С. 56–58.

68. **Рекомендации** по акустическому благоустройству шумных помещений ИВЦ и МСС. Научно-исследовательский институт Госстроя СССР. — Киев, 1974.— 45 с.

69. **Рембовский А.М.** Комплексы радиоконтроля и выявления каналов утечки информации от ЗАО «Иркос» — состояние и перспектива // Системы безопасности связи и телекоммуникаций. 1998. № 23. С. 54–57.

70. **Руденко В.М., Халяпин Д.Б., Магнушевский В.Р.** Малошумящие входные цепи СВЧ приемных устройств. — М.: Связь, 1971. — 279 с.

71. **Руководство** по расчету и проектированию звукоизоляции ограждающих конструкций зданий. — М.: Стройиздат, 1983.

72. **Семёнов А.Б.** Волоконно-оптические подсистемы современных СКС М.: Академия АйТи: ДМК Пресс, 2007. — 632 с.

73. **Системы** «Спрут» и «Ольха» // Системы безопасности связи и телекоммуникаций. 1998. № 19. С. 76–77.

74. **Скребнев В.И.** Подповерхностная локация: новые возможности // Специальная техника. 1998. № 1. С. 9–11.

75. **Снижение** шума в зданиях и жилых районах / Под ред. Г.А. Осипова, Е.Я. Юдина. — М.: Стройиздат, 1987. — 548 с.

76. **Специальная** техника: Каталог. — М.: ЗАО «SET-1», 1998. — 90 с.

77. **Специальная** техника: Каталог. — М.: НПО «Защита информации», 1996. — 56 с.

78. **Специальная** техника: Каталог. — М.: Прогресс-тех, 1996. — 79 с.

79. **Специальные** технические средства: Каталог. — М.: Гротек, 1998. — 33 с.

80. **Специальные** технические средства: Каталог. — М.: Маском, 2002.

81. **Специальные** технические средства: Каталог. — М.: NOVO, 2003. — 15 с.

82. **Специальные** технические средства: Каталог. — М.: Элвира, 1998. — 43 с.

83. **Средства** защиты информации от утечки по техническим каналам. Каталог продукции. Санкт-Петербург: 2000. — 37 с.

84. **Сталенков С.Е., Шулика Е.В.** НЕЛК — новая идеология комплексной безопасности. Способы и аппаратура защиты телефонных линий // Защита информации. «Конфидент». 1998. Сентябрь-октябрь; 1999. Январь-февраль.

85. **Сударев И.В.** Криптографическая защита телефонных сообщений // Специальная техника. 1998. № 2. С. 47–54.

86. **Съем** информации по виброакустическому каналу (экспертная группа компании «Гротек») // Системы безопасности связи и телекоммуникаций. 1995. № 5. С. 12–15.

87. **Терминология** в области защиты информации: Справочник. — М.: ВНИИ «Стандарт», 1993. — 110 с.

88. **Проспекты** фирм «СмерШ Техникс», «НЕРА-С», ИКМЦ-1, STTGroup, «Защита информации», «Мир безопасности», «Иркос», АОХК «Электрозавод» (Лаборатория № 11), НОВО, «Сюртель» на выставках «Безопасность», 1996–2014 гг.

89. **Технические** средства защиты информации: Каталог. — М.: ЗАО «Анна». Техника специального назначения: Каталог-2014. — 23 с.

90. **Технические** системы защиты информации: Каталоги. — М.: ЗАО НПЦ «Нелк», 1997 —2014. гг.

91. **Технические** средства видовой разведки. Под ред. А.А. Хорева. — М.: РВСН, 1997. — 327 с.

92. **Технические** средства разведки. Под ред. В.И. Мухина. — М.: РВСН, 1992. — 335 с.

93. **Томас Харви Джонс.** Обзор технологии нелинейной радиолокации // Системы безопасности связи и телекоммуникаций. 1996. № 26. С. 34–36.

94. **Томас Харви Джонс.** Обзор технологии нелинейной радиолокации. Специальная техника. 1998. № 4–5. С. 27–32.

95. **Топоровский П.В.** Средства нелинейной радиолокации. Реальный взгляд // Системы безопасности связи и телекоммуникаций. 1998. № 23. С. 94–97.

96. **Торокин А.А.** Основы инженерно-технической защиты информации. — М.: Ось-89, 1998. — 336 с.

97. **Торокин А.А.** Инженерно-техническая защита информации. Учебное пособие — М.: Гелиос АРВ, 2005. — 960 с.

98. **Фролов Г.П.** Тайны тайнописи. — М.: АО «Безопасность», 1992.

99. **Халяпин Д.Б.** Акустическая защита выделенного помещения // Мир безопасности. 1997. № 12. С. 41–44.

100. **Халяпин Д.Б.** Акустоэлектрические, акустопреобразовательные каналы утечки информации и возможные способы их подавления // Мир безопасности. № 5. С. 47–53.

101. **Халяпин Д.Б.** Вас подслушивают? Защищайтесь! — М.: Боярд, 2004. — 432 с.

102. **Халяпин Д.Б.** Визуально-оптический канал утечки информации // Мир безопасности. 1998. № 7. С. 48–50.

103. **Халяпин Д.Б.** Как устроены «клопы» // Частный сыск. Охрана. Безопасность. 1995. № 11.

104. **Халяпин Д.Б.** Коаксиальные и полосковые фильтры сверхвысоких частот. — М.: Связь, 1969. — 64 с.

105. **Халяпин Д.Б.** Комплексная защита информации // Сборник статей. Отделение погранологии Международной Академии информатизации. Вып. 5. Ч. 1. — М.: МАИ, 1998. — С. 109–113.

106. **Халяпин Д.Б.** Предают обычно свои // Мир безопасности. 1997. № 8. С. 29–30.

107. **Халяпин Д.Б.** Стены и уши. Защита информации // Мир безопасности. 1998. С. 76–81.

108. **Халяпин Д.Б.** Физические основы возникновения вибрационного (структурного) канала утечки информации и возможности его подавления // Мир безопасности. 1999. № 2. С. 42–48.

109. **Халяпин Д.Б.** Чем заткнуть «длинное ухо» // Мир безопасности. 1998. № 3. С. 46–49.

110. **Халяпин Д.Б.** Что необходимо защищать, когда защищаешь информацию // Мир безопасности. 1998. № 1. С. 46–49.

111. **Халяпин Д.Б., Тарасов И.Л.** Выделенное помещение с обеспечением визуального контроля // Международная конференция по информатизации правоохранительных органов. Тезисы докладов. Ч. 2. — М.: Академия МВД РФ, 1998. С. 167–168.

112. **Халяпин Д.Б., Терентьев Е.Б.** Возможные источники и каналы утечки информации из телефонных линий связи // Международная конференция по информатизации правоохранительных органов. Тезисы докладов. Ч. 2. — М.: Академия МВД РФ, 1998. С. 165–167.

113. **Халяпин Д.Б., Шерстнева Ю.Л.** Защита информации, обрабатываемой ПЭВМ и ЛВС, от утечки по сети электропитания // Системы безопасности связи и телекоммуникаций. 1999. № 28. С. 70–71.

114. **Халяпин Д.Б., Шерстнева Ю.А.** Определение предельной величины опасного сигнала, наводимого ПЭВМ и ЛВС в сеть электропитания // Системы безопасности связи и телекоммуникаций. 1999. № 2. С. 30–32.

115. **Халяпин Д.Б., Ярочкин В.И.** Основы защиты информации: Учебное пособие. — М.: ИПКИР, 1994. — 123 с.

116. **Хорев А.А**. Техническая защита информации. Т. I. Технические каналы утечки информации: Учебное пособие. — М.: НПЦ «Аналитика», 2008. — 436 с.

117. **Хорев А.А**. Защита информации от утечки по техническим каналам. Ч. I. Технические каналы утечки информации: Учебное пособие. — М.: Гостехкомиссия России, 1998. — 320 с.

118. **Хорев А.А.** Техническая защита информации: Учебное пособие для студентов вузов. — М.: НПЦ «Аналитика», 2008. — 436 с.

119. **Хорев А.А.** Технические средства и способы промышленного шпионажа. — М.: ЗАО «Дальснаб», 1997. — 230 с.

120. **Хоффман Л.Д.** Современные методы защиты информации. — М.: Советское радио, 1980.

121. **Центр** речевых технологий. Интерактивная программа обработки речевых сигналов. Каталог, 1999. — 15 с.

122. **Щербаков Г.Н.** Применение нелинейной радиолокации для дистанционного обнаружения малоразмерных объектов // Специальная техника. 1999. № 6. С. 34–39.

123. **Энциклопедия** промышленного шпионажа / Ю.Ф. Которин, Е.В. Куренков, А.В. Лысов, А.Н. Остапенко. — С-Пб.: Полигон, 1999. — 512 с.

124.**Яковлев А.В.** Волоконно-оптическая система передачи конфиденциальной информации // Электросвязь. 2009. № 10.

125. **Ярочкин В.И.** Технические каналы утечки информации. — М.: ИПКИР, 1994.— 106 с.

126. **Ярочкин В.И.** Система безопасности фирмы. — М.: Ось-89, 2003. — 352 с.

Оглавление